



# TRABAJO FIN DE GRADO

## RÉGIMEN JURÍDICO DEL DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA Y SU RELACIÓN CON LA NUEVA NORMATIVA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.

LEGAL REGIME OF THE RIGHT OF ACCESS TO PUBLIC INFORMATION AND ITS RELATIONSHIP WITH THE NEW REGULATION OF PROTECTION OF PERSONAL DATA.

### GRADO EN DERECHO

Facultad de Ciencias Jurídicas  
UNIVERSIDAD DE ALMERÍA

Curso académico: 2014/2018

Almería, junio de 2018



Tutor: D. Lorenzo Mellado Ruiz

Autora: Eva Rodríguez García



### RESUMEN:

Mi trabajo señala que el objetivo de la protección de datos es el equilibrio entre la libre circulación de la información y la salvaguarda de la intimidad, junto con el cumplimiento del deber de publicidad de las Administraciones Públicas. Dentro de los derechos que las personas ostentamos para el control de nuestros datos está el derecho de acceso, éste nos aporta la capacidad de solicitar información que sea de nuestro interés siempre que no entre en conflicto con los límites impuestos por la ley para la seguridad del Estado y la protección de terceros. Las empresas privadas también tienen que cumplir con este derecho y otros como los derechos ARCO y los nuevos derechos al olvido y a la portabilidad. El objetivo es hacer más reales y comprensibles los cambios que se están llevando a cabo en cuanto a protección de datos, conocer cómo se materializa el cumplimiento del Reglamento General de Protección de Datos 2016/679 en España y la forma en que podemos ejercitar los derechos que nos brinda.

### SUMMARY:

My final degree project indicates that the objective of data protection is the balance between the free circulation of information and the safeguarding of privacy, together with compliance with the duty of public administrations. Among the rights that we hold for the control of our data is the right of access, this gives us the ability to request information that is of our interest as long as it does not conflict with the limits imposed by law for the security of the State and third party protection. Private companies also have to comply with this right and others such as ARCO rights and new rights to oblivion and portability. The objective is to make the changes that are being carried out in terms of data protection more real and understandable, to know how compliance with the General Data Protection Regulation 2016/679 in Spain and the way in which we exercise our rights is materialized. what it gives us.

**Abreviaturas    Significado**

AEPD	Agencia Española de Protección de Datos.
ALOPD	Anteproyecto de Ley Orgánica de Protección de Datos.
ARCO	Acceso, rectificación, cancelación y oposición.
CE	Constitución Española.
CTBG	Consejo de Transparencia y Buen Gobierno.
INAP	Instituto Nacional de Administración Pública.
LOPD	Ley Orgánica de Protección de Datos.
LORTAD	Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de carácter personal.
LPAC	Ley del Procedimiento Administrativo Común de las Administraciones Públicas.
LRJAP	Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
LTBG	Ley de Transparencia, acceso a la información pública y Buen Gobierno.
LTPA	Ley de Transparencia Pública de Andalucía.
RGPD	Reglamento General de Protección de Datos de la Unión Europea.
RLOPD	Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos.
STC	Sentencia del Tribunal Constitucional.
UE	Unión Europea.

## ÍNDICE:

1. INTRODUCCIÓN .....	4
2. APROXIMACIÓN AL MARCO REGULADOR ACTUAL DEL DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA.....	7
a) Bases constitucionales .....	7
b) Caracterización del derecho de acceso en la legislación básica vigente y notas fundamentales sobre su régimen jurídico .....	9
c) Principios rectores del derecho de acceso .....	15
3. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y PUBLICIDAD PASIVA .....	16
a) Notas básicas de la evolución comunitaria de la normativa sobre protección de datos de carácter personal.....	16
b) Novedades que aporta el Reglamento General de Protección de Datos 2016/679 .....	19
c) Grupo normativo interno actual o vigente .....	24
4. EJERCICIO DEL DERECHO DE ACCESO Y LÍMITES DERIVADOS DE LA TUTELA DE DATOS PERSONALES .....	27
a) Procedimiento.....	28
b) Denegación de acceso e información de acceso limitado.....	33
c) Inadmisión de acceso .....	37
CONCLUSIONES .....	40
BIBLIOGRAFÍA.....	42

## **1. INTRODUCCIÓN**

En este TFG analizo la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos (en adelante LOPD), que será sustituida por el Anteproyecto de Ley Orgánica de Protección de Datos de 26 de octubre de 2017 (en adelante ALOPD), junto con el estudio de la Ley 19/2013, de 9 de diciembre, de Transparencia, acceso a la información pública y Buen Gobierno (en adelante LTBG), y destaco el Reglamento General de Protección de Datos de la Unión Europea 2016/679 de 27 de abril (en adelante RGPD) del Parlamento europeo y del Consejo, además de señalar su evolución histórica, sus objetivos y su método de aplicación en España al ser traspuesto (aunque la transposición no es obligatoria en el caso de los reglamentos ya que son de aplicación directa y obligatorios en todos sus elementos para todos los Estados Miembros, pero al colisionar con algunas de las normas españolas que regulaban esta materia el legislador se ha visto obligado a la elaboración de una nueva ley orgánica).

Introduzco por tanto un tema de plena actualidad, la protección de datos de carácter personal. La particularidad de éste es que además está estrechamente relacionado con las practicas curriculares que he realizado en la Excelentísima Diputación de Almería sobre la adaptación del RGPD al funcionamiento de las Administraciones Públicas españolas y es que, aunque los Reglamentos europeos no necesitan adaptación por ser directamente aplicables, en el caso de España contravenía la LOPD que regulaba esta materia, por ello se está actuando por parte del legislador para la elaboración del nuevo Anteproyecto de Ley Orgánica de Protección de Datos y así poder cumplir con las disposiciones de la Unión Europea. Mis prácticas externas se han basado en cambiar el modo de operar de la Diputación intentando ser lo más respetuoso posible con su versión anterior para que este hecho no entorpezca su funcionamiento normal pero haciendo cumplir el RGPD y además enseñarles a los funcionarios que allí trabajan cuáles serán los pasos a seguir para continuar en este camino en el momento que el RGPD entre en vigor y así orientarlos. Además esta es una materia nueva para mí ya que es relativamente reciente y no se incluye en los estudios del grado, por lo que me ha supuesto un trabajo de investigación más intenso.

La protección de datos no restringe la libertad para recoger datos personales y utilizarlos para diferentes finalidades, siempre y cuando sean lícitas y estén claramente especificadas al interesado para que pueda prestar su consentimiento, sino que se preocupa por imponer a quienes los recaban ciertos requisitos que aporten seguridad a los afectados. Así se otorga a los ciudadanos un poder de control sobre sus propios datos y se protegen sus derechos y libertades fundamentales. Se pretende mantener la existencia de libre circulación de los datos ya que nos encontramos en un mundo globalizado pero aportando siempre un mínimo de seguridad a éstos.

Por otro lado, la protección de datos es también un límite a la libertad de información, ya que hay ciertos datos que el legislador no permite compartir, o al menos, pone más trabas para ello, porque suponen un riesgo. Existe también otra clase de límites a la recogida de datos impuestos por la protección de datos como el requisito del consentimiento, la previa información del tratamiento que van a recibir, etc.

Una parte de la protección de datos es el derecho de acceso a los mismos, que a su vez, está ligado con la transparencia de las Administraciones Públicas. El derecho de acceso se encuentra recogido en la Constitución Española (en adelante CE) aprobada por las Cámaras el 31 de octubre de 1978, aunque no como Derecho Fundamental, no se encuentra tampoco explícitamente el derecho a la protección de los datos personales pero se entiende que está integrado dentro del Derecho Fundamental al honor, la intimidad personal y familiar y la propia imagen, por ello que la protección de datos se desarrolle como una Ley Orgánica y el derecho de acceso como una parte de éste y de la transparencia de las Administraciones.

En el plano europeo dentro de los derechos que regula el RGPD para el ejercicio de los interesados encontramos el derecho de acceso. Con él, los ciudadanos tenemos el derecho tanto a conocer información propia, datos de carácter personal, expedientes administrativos o actividades de tratamiento, como a conocer la información pública, la cual se ha hecho mucho más visible en nuestro país por las imposiciones de la LTBG, cuya creación está influenciada por anteriores disposiciones de la UE como la Directiva 95/46/CE (24 de octubre de 1995) del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y

a la libre circulación de estos datos. En esta Ley se obliga a incrementar la publicidad de los organismos públicos por sus responsables y por lo tanto a garantizar el acceso a la información por los interesados, según nos señala el RGPD, a partir de ahora la información se otorga al interesado en capas, la primera se da por ejemplo al rellenar el formulario de petición de información, es decir, al ejercitar el derecho de acceso (se le facilitan los datos de contacto del delegado de protección de datos, cuál será el tratamiento de sus datos etc.) y la segunda, una vez que se concede la petición de información concreta que ha realizado el interesado. El derecho de acceso, en conclusión, nos permite acceder a una información más detallada.

Los principios básicos del derecho de acceso son que la información debe ser accesible, la manera de solicitarla intuitiva y, en general, gratuito. Una vez otorgada debe ser comprensible para el interesado y sobre todo, es muy importante que se cumpla la interoperabilidad tanto entre Administraciones Públicas entre sí como con el ciudadano para agilizar los trámites y dar un cumplimiento efectivo a este derecho.

Por último, uno de los requisitos más importantes para que el tratamiento de la información sea adecuado es utilizar los sistemas de seguridad oportunos (seudonimización, codificación, encriptación, etc.), es decir, evitar por todos los medios que una persona ajena a la información, es decir, que no sea ni el interesado ni la persona que trata los datos pueda acceder a ellos provocando una mella en su seguridad y pudiendo así conocerlos o incluso distribuirlos. De todo ello se encarga el responsable del tratamiento, esta es la figura de la persona cuya función es recoger los datos y tratarlos, el responsable a su vez puede delegar sus tareas al encargado del tratamiento, que es una figura que bien se utiliza para descongestionar de tareas al responsable o bien porque está más especializado, puede ser tanto un organismo público como uno privado. Pero por encima de ellos siempre se encuentra la nueva figura del delegado de protección de datos, los datos de éste se encuentran en el formulario de consentimiento que el interesado debe firmar cuando cede sus datos y será ante quien se pedirá responsabilidad si hay problemas con la seguridad y los datos se ven afectados.

Los ciudadanos contamos también con otros derechos como: el derecho a rectificar la información aportada (ya que debe estar siempre actualizada), el derecho a la cancelación de los datos (derecho al olvido), el derecho de oposición (archivar ciertas informaciones),

el derecho a la portabilidad de los datos (movimiento de los datos de un responsable de tratamiento a otro), el derecho de limitación de uso, etc.

Hay que hacer especial referencia a la necesidad, no sólo de que estos derechos existan, sino de que los ciudadanos sepan cómo ejercitarlos, cuál es su procedimiento, sus límites, qué pueden hacer en el caso de que no se cumpla la tutela que el ordenamiento jurídico otorga a la protección de sus datos y, en definitiva, que esté debidamente informado, de forma clara y sencilla, y así protegidos sus derechos y libertades fundamentales.

## **2. APROXIMACIÓN AL MARCO REGULADOR ACTUAL DEL DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA**

### **a) Bases constitucionales**

El derecho constitucional en el que se basa el legislador para desarrollar el derecho de acceso a la información pública se encuentra recogido en la CE en su artículo 105.b)<sup>1</sup>. En éste, la Constitución señala que los ciudadanos podrán acceder a la información que deseen, siempre y cuando no afecte, ni a la seguridad y defensa del Estado, ni a la averiguación de los delitos y la intimidad de las personas. Es decir, tiene ciertos límites (que abarcaremos más adelante) ya que hay que tener en cuenta el respeto a los derechos fundamentales de otras personas, además de sus bienes e intereses públicos protegidos. Al contenerse fuera del Título I es un derecho constitucional de configuración legal y no un derecho fundamental, lo cual confronta con la doctrina del Tribunal Europeo de los Derechos Humanos.

En el articulado de la CE no encontramos un derecho que señale expresamente el derecho a la protección de datos, ello en mi opinión provoca un pequeño desamparo respecto al control de la información que existe sobre nosotros mismos. El apartado cuarto del artículo 18 de la CE señala lo más parecido a la protección de datos que podemos encontrar en la ley fundamental y es el derecho a la autodeterminación informativa, según Pérez Royo, esta norma lo que pretende es que el legislador limite el uso de la informática para garantizar ciertos derechos fundamentales de los ciudadanos como el honor y la

---

<sup>1</sup> Véase PÉREZ ROYO, J., Lección 12 “Los derechos constitutivos de la personalidad: honor, intimidad y propia imagen” páginas 311 a 313, lección 13 “Los derechos de la comunicación física, intelectual y social: libertad de expresión” páginas 320 a 324, en Curso de Derecho Constitucional, Madrid, 2016.

intimidad personal y familiar. La respuesta que da nuestro país a este problema es la creación de agencias de control, como la Agencia Española de Protección de Datos (en adelante AEPD) y la elaboración de la LOPD que desarrollaré en las próximas páginas. Por otra parte, este artículo con el paso del tiempo se ha consolidado en la jurisprudencia española como un derecho fundamental de la protección de datos aunque no se le llame así expresamente<sup>2</sup>.

El derecho de acceso, se relaciona a su vez con el artículo 20.1.d) CE, el derecho de información, es decir, el derecho de comunicación intelectual, de transmitir y recibir libremente información veraz sea cual sea el medio que lo difunde. Por último, también tiene cierta relación con el artículo 23 CE de participación de los ciudadanos en los asuntos públicos propios de nuestro sistema democrático.

El derecho de acceso recogido en nuestra Constitución da la justificación a la imposición de que las Administraciones Públicas deben ser transparentes, lo cual está regulado en la LTBG, además la función principal de éstas es servir a los ciudadanos, por lo que, toda información que generen y posean les pertenece. Es un derecho reconocido a nivel internacional debido a la naturaleza representativa de los gobiernos democráticos.

Como límite a este derecho, existe la protección de datos, que tiene por objeto proteger la intimidad de las personas físicas, además de otros derechos (derecho a la dignidad, a la intimidad personal y familiar, al honor, etc.), frente al riesgo que para las personas supone la recopilación y el uso indiscriminado de sus datos personales.

En mi opinión, sería importante que la CE recogiera de forma más clara y uniforme un derecho fundamental de los ciudadanos de protección de sus datos ya que el derecho de acceso está creado a consecuencia de la gran cantidad de datos personales que hay esparcidos en la sociedad de la información, y por tanto a consecuencia de la protección de datos, y sin embargo está desarrollado de forma más clara (en un solo artículo) que lo que para mí es el origen de todo ello, la protección de datos.

---

<sup>2</sup> Según la STC 292/2000, FJ 6º, “el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, su uso y su destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado”. Protege por tanto frente al uso injustificado y no autorizado de los datos personales por procedimientos automatizados, ya sean datos de naturaleza íntima o no.



Encontramos varias referencias a la protección de los datos personales en diferentes artículos y en la jurisprudencia del Tribunal Constitucional que consolida su existencia pero no como un derecho fundamental específico que quede claro a aquellos que no se dediquen a la rama jurídica, lo cual provoca una indefensión, sino que existe como un sub apartado de un derecho fundamental más grande, el derecho al honor, la intimidad personal y familiar y la propia imagen.

#### **b) Caracterización del derecho de acceso en la legislación básica vigente y notas fundamentales sobre su régimen jurídico**

El derecho de acceso viene regulado por el RGPD y por la LOPD y consiste en la capacidad del ciudadano para conocer el uso que los organismos hacen de sus datos de carácter personal (a quiénes dan su información, qué categorías de datos están recogidas, si hay transmisiones de datos internacionales o si están siendo cedidos a terceros, para qué se utilizan, cual es el origen de los datos, etc.) En todo caso la información debe proporcionarse de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo. Este derecho tiene la función principal de ejercer un control sobre las actuaciones de la Administración.

Se define el concepto dato de carácter personal como cualquier información concerniente a personas físicas identificadas o identificables. Se considera persona física identificable cualquiera cuya identidad pueda determinarse, directa o indirectamente, mediante un identificador, por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea, elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona. Este concepto sólo abarca los datos de personas físicas, y no, en cambio, los datos de personas jurídicas, como empresas, sociedades, instituciones, etc.

Como ya he dicho, el artículo 105 b) de la CE provoca que los ciudadanos tengan acceso a la información, gracias a las diferentes leyes que desarrollan lo que ya señala la ley fundamental, existen varios tipos de acceso a la información:

**- El derecho de acceso de los interesados a los expedientes administrativos, regulado por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante LPAC)<sup>3</sup>.**

Esta ley regula en su artículo 53.a) el derecho a conocer el estado de la tramitación del procedimiento en los que formen parte como interesados. Por supuesto, éste debe ser información personal, no se puede acceder a información de terceros. El derecho de acceso es personalísimo, en este caso, se trata de que una persona interesada reclama a la Administración Pública una información sobre sí mismo en un proceso administrativo de la que dispone la Administración Pública de forma más detallada.

Se otorga al interesado el derecho de conocer en cada momento el estado de la tramitación de los procedimientos (de los que formen parte), el sentido del silencio administrativo, el órgano al que le compete, los actos dictados y a obtener copia de ello. Se refiere, en conclusión, a la situación del interesado con uno o varios procedimientos administrativos.

Por otra parte, la LPAC da también la oportunidad de acceder a los archivos y registros de las Administraciones Públicas<sup>4</sup>, según dispone su artículo 13 d), esto es la información que forme parte de un expediente pero se encuentre en archivos administrativos (sea cual sea su formato) de las administraciones territoriales (del Estado, CCAA y Locales) o de otras entidades de derecho público vinculadas o dependientes de las administraciones pero cuya funcionalidad sea administrativa, con el requisito de que estén finalizados los procedimientos a los que corresponden cuando sean requeridos. Se puede acceder a ellos directamente o solicitar copia de estos.

**- El derecho de acceso a la información pública, regulado por la Ley 19/2013, de 9 de diciembre, de Transparencia, acceso a la información pública y Buen Gobierno.**

La LTBG por otro lado, separa la información pública en dos elementos, la publicidad activa que es la imposición que hace la LTBG en su artículo 5 a las diferentes sedes electrónicas o páginas webs de las Administraciones Públicas y otros organismos de publicar de forma permanente, periódica y actualizada la información que sea relevante

---

<sup>3</sup> Véase BALLESTEROS, R., “Nueva Ley 39/2015 y derecho de acceso a los expedientes administrativos” en Actualidad jurídica Aranzadi, nº 923, 2016.

<sup>4</sup> Véase SOTO LOSTAL, S., Capítulo III “Derecho de acceso a la información de los archivos y registros de la Administración Pública”, Capítulo IV “Derecho de acceso a los archivos y registros administrativos como especialidad del derecho a recibir información veraz por cualquier medio de difusión” en Derecho de acceso a la información, Valencia, 2011.

para garantizar tanto la transparencia de su actividad como un control de la actuación pública por parte de los ciudadanos, ello se realiza tanto en el ámbito de la Administración General del Estado como en las Administraciones de las Comunidades Autónomas en un Portal de Transparencia donde se recoge la información señalada como obligatoria en la LTBG y la que es solicitada más frecuentemente proporcionando así información relevante para el interés de la ciudadanía. El control del cumplimiento de esta obligación por parte del Estado vendrá dada por parte un órgano autónomo, el Consejo de Transparencia y Buen Gobierno que detallaré en las páginas siguientes. Y el derecho de acceso<sup>5</sup>, éste es de titularidad universal pero se debe tener un interés legítimo para acceder a ciertos tipos de información, aunque no es obligatorio motivar la petición. En conclusión, consiste en la petición de cualquier ciudadano que quiera solicitar y obtener información de su interés, con los límites que señale la ley, relacionada con la Administración y sus actuaciones, que no esté ya publicada en los mencionados portales de transparencia (artículo 12 LTBG). Además, nuestro legislador da la posibilidad a los ciudadanos de que puedan hacerse cargo de sus propios datos recogidos por las Administraciones, protegerlos, revisarlos y utilizando otros derechos, también regulados por la Ley, rectificarlos, suprimirlos, oponerse, limitar su tratamiento etc.

La transparencia es entendida en general como la obligación de la Administración de mostrar a los ciudadanos, que son sus interesados, su actividad pero además de eso, no debemos olvidar que existe transparencia en muchos ámbitos, por ejemplo, cuando se recaban los datos se tiene que dar al interesado toda la información necesaria como los datos de contacto del responsable y el delegado de protección de datos, también cuando se tratan, ya que el interesado debe conocer en todo momento la finalidad y los usos, cesiones etc. o, si hay una brecha de seguridad ya que hay que informar de qué es lo que ha ocurrido, así lo explican en las jornadas realizadas en el Instituto Nacional de Administración Pública (en adelante INAP) llamadas "Proceso para la adaptación al reglamento general de protección de datos en las Administraciones públicas" a las que

---

<sup>5</sup> Véase GAMERO CASADO, E., FERNÁNDEZ RAMOS, S., MORA RUIZ, M., Tema 11 "El estatuto del ciudadano. La posición jurídica del ciudadano: transparencia y acceso a la información pública, el derecho de protección de los datos personales", páginas 222 a 226 y 229 a 232, en Derecho Administrativo para estudios no jurídicos, Madrid, 2016.

asistieron diferentes representantes de las administraciones del país para conocer más a fondo el tema de la protección de datos<sup>6</sup>.

El ámbito objetivo del derecho de acceso es la información pública que el ciudadano puede pedir, consta en documentos o contenidos, cualquiera que sea su formato, que obran en poder de algunos de los sujetos que integran las Administraciones Públicas y que hayan sido adquiridos o elaborados en el ejercicio de sus funciones (artículo 13 LTBG)<sup>7</sup>. Siempre debe ser información que ya exista, es decir, que no esté en elaboración y que, por supuesto, no se refiera a consultas jurídicas o peticiones de dictámenes. Por otro lado, no sólo se considera información pública a los documentos creados por Administraciones Públicas, sino también los documentos que hayan producido los administrados como solicitudes, propuestas, reclamaciones etc. Existe una exclusión de información que puede ser solicitada (artículo 18.1.b) LTBG), es la información auxiliar o de apoyo como borradores, notas, comunicaciones internas etc. Esto es así porque esta información es simplemente de organización interna de la Administración y no tiene nada que ver con la información que los ciudadanos solicitan. Además de existir una serie de límites a este derecho justificados por la protección de derechos y principios constitucionales.

Por otro lado, el ámbito subjetivo del derecho de acceso es la determinación de quienes deberán aplicarlo<sup>8</sup>, según los artículos 2 y 3 de la LTBG será de obligatorio cumplimiento para la Administración General del Estado, las Administraciones de las Comunidades Autónomas y de Ceuta y Melilla y las entidades que integran la Administración Local, entidades gestoras y los servicios comunes de la Seguridad Social, organismos autónomos, las Agencias Estatales, las entidades públicas empresariales y entidades de Derecho Público, entre ellas las Universidades públicas. También las corporaciones de Derecho Público, la Casa de su Majestad el Rey, el Congreso de los Diputados, el Senado,

---

<sup>6</sup> Véase Jornada INAP "Proceso para la adaptación al reglamento general de protección de datos en las Administraciones públicas": <http://laadministracionaldia.inap.es/noticia.asp?id=1508414>

<sup>7</sup> Véase CAZURRO BARAHONA, V., "Introducción a la protección de datos personales" puntos 3 y 4, en Grandes Tratados. Practicum protección de datos 2015, BIB 3509, enero 2014.

<sup>8</sup> Véase PORTAL DE TRANSPARENCIA (Gobierno de España), "Guía para el ciudadano del derecho de acceso a la información". Disponible en: <http://transparencia.gob.es/transparencia/dam/jcr:eb071b8f-7982-4518-b102-d2a4f5f51640/guia-del-ciudadano.pdf>

Véase artículo 2 Ley 19/2013, de 9 de diciembre, de Transparencia, acceso a la información pública y Buen Gobierno.

el Tribunal Constitucional y el Consejo General del Poder Judicial, así como el Banco de España, el Consejo de Estado, el Defensor del Pueblo, el Tribunal de Cuentas, el Consejo Económico y Social y las instituciones autonómicas análogas, aunque la única información que están obligados a aportar es la que tenga que ver con sus actividades relacionadas con derecho administrativo. Por otro lado, las sociedades mercantiles en cuyo capital social la participación, directa o indirecta, de las entidades previstas en este artículo sea superior al 50 por 100. Las fundaciones del sector público previstas en la legislación. Y las asociaciones en la medida en que, por su peculiar naturaleza y por carecer de una estructura administrativa propia, le resulten aplicables estas disposiciones. Además de otros sujetos obligados como los partidos políticos, organizaciones sindicales y organizaciones empresariales y las entidades privadas que perciban durante el período de un año ayudas o subvenciones públicas en una cuantía superior a 100.000 euros o cuando al menos el 40 % del total de sus ingresos anuales tengan carácter de ayuda o subvención pública, siempre que alcancen como mínimo la cantidad de 5.000 euros. Sin embargo, según su artículo 3 los partidos políticos, organizaciones sindicales y organizaciones empresariales, así como entidades privadas que perciban subvenciones públicas en los términos fijados por la Ley no están sujetos a esta obligación de atender al derecho de acceso.

En la ley se recogen los principios en el ámbito técnico que rigen la publicidad activa, en estos se aclara que la información debe ser proporcionada de una forma accesible e intuitiva, lo que significa que todas las personas deben poder llegar a ella fácilmente, no se deben utilizar demasiados tecnicismos y debe estar a la vista de cualquiera, además debe existir interoperabilidad, es decir, que sea fácil el intercambio de información entre las Administraciones entre sí como con los ciudadanos para conseguir una cooperación propia de la sociedad de la información y así evitar obstáculos que dificulten la consecución de este derecho y por último, la información debe ser otorgada de manera que se pueda reutilizar, por ello, una de las medidas que se han creado es que las consultas más frecuentes de los ciudadanos son publicadas en los portales de transparencia para no tener que responder repetidamente a las mismas dudas y ser eficientes.

Encontramos en el articulado del ALOPD el artículo 14 en el cual se regula el Derecho de acceso que viene relacionado con el artículo 15 del RGPD<sup>9</sup>. En él, el legislador trata de especificar las condiciones para ejercitar este derecho en España. El afectado podrá solicitar la información al responsable, si éste cuenta con una gran cantidad de información del interesado y solo necesita una información en concreto podrá especificar si solicita todos sus datos personales o sólo una parte específicamente. El derecho de acceso se considerará cumplido si el responsable concede al afectado un sistema de acceso remoto, directo y seguro a los datos.

El afectado según nos señala el artículo 22 de la LTBG podrá elegir el medio en el que quiere que se le transmita la información, acarreando ello posibles costes según el medio elegido, por ejemplo es gratuita si se otorga por la vía general que es la electrónica, pero puede tener un coste si quiere que se le envíe por correo postal ya que conlleva la necesidad de imprimir los datos, enviarlos etc. El coste será siempre proporcional.

Otra de las características más novedosas del derecho de acceso es que el afectado tiene derecho a conocer cuál es el plazo de conservación de sus datos y como novedad aportada por el RGPD si no es posible determinarlo, habrá que comunicarle cuáles van a ser los criterios utilizados para determinar su eliminación. Por ejemplo, en el caso de que una Administración conste con datos personales y no sepa el momento exacto en el que serán eliminados porque no hay un plazo riguroso, se deberá informar al solicitante de que la supresión de esta información se llevará a cabo, por ejemplo, cuando resulte completada la finalidad para la que fueron recogidos y para la cual él dio su consentimiento expreso.

En base a nuestra Constitución, artículo 105,b), pueden ejercer este derecho tanto personas físicas como jurídicas, aunque en este caso se le puede solicitar que aporten cierta documentación para verificar su validez e identidad.

La información puede estar limitada, lo cual desarrollaré más adelante, pero en el caso de que un ciudadano solicite una información cuya limitación es parcial, se le puede dar acceso a la parte restante de ésta tal y como especifica la LTBG en su artículo 14.

---

<sup>9</sup> Véase RUBIO TORRANO, E., “El Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal” en Revista doctrinal Aranzadi Civil-Mercantil, nº 1, 2018.

Una de las características fundamentales del derecho de acceso en el RGPD y que se prevé que se recoja la futura LOPD es que nos encontramos ante un modelo de información por capas, es decir, que se amplía de forma considerable la cantidad de información que hay que otorgar, además ahora la información que la Administración tiene en su poder se presenta ante los ciudadanos por niveles. En un primer nivel se presenta la información básica de forma resumida, en el momento que el interesado rellena los datos que se le piden se le informará en el medio en el que se recojan los datos sobre la identificación del responsable del tratamiento, la finalidad del tratamiento, la ley que legitima su tratamiento, los derechos que puede ejercitar, si se utilizan para la realización de perfiles y el origen de los datos en el caso de que estos hayan sido obtenidos por persona distinta al interesado, por ejemplo si han sido cedidos por otra Administración Pública o por terceros. En un segundo nivel se aportará la información adicional de una forma más detallada, este es el momento en el que se ejercita el derecho de acceso. El modelo de información por capas es muy fácil de cumplir mediante un formulario electrónico ya que al interesado se le puede dar toda la información de manera más ágil solo redirigiéndole a un enlace, pero también se tendrá que dar en los formatos en papel.

### **c) Principios rectores del derecho de acceso**

Los principios que rigen el funcionamiento de este derecho son: es un derecho de todos (artículo 3 LPAC), cualquier ciudadano que tenga capacidad de obrar puede ejercitarlo y solicitar tanto información propia que le resulte de interés, como información pública que no esté publicada, por tanto pueden solicitar información tanto personas físicas como personas jurídicas. En el caso de que el derecho se ejercite para acceder a datos íntimos, expedientes administrativos etc., el derecho es personalísimo, no se puede acceder a información de terceros a menos que éste haya dado permiso explícito o que la información ya haya sido publicada por él mismo (artículo 15 LTBG).

Este derecho se aplica a todas las entidades públicas, se puede solicitar en cualquiera de ellas, las empresas privadas si recogen datos personales del interesado también están obligadas a permitirle el ejercicio del derecho de acceso, entre otros, además de tener que cumplir otras imposiciones del RGPD como la llevanza de un registro de actividades de tratamiento (artículo 30) o la designación de un delegado de protección de datos (artículo

37) si estas cumplen los requisitos de tener más de 250 empleados o manejar un gran volumen de datos o datos sensibles (Considerando nº 13).

Los funcionarios tienen el deber de colaborar con los ciudadanos, ya que aunque existe la posibilidad de solicitar estos datos por vía electrónica, puede hacerse también en la propia Administración y siempre debe ser sencillo, ágil y gratuito. Los organismos de la Administración deben establecer mecanismos accesibles para el ejercicio de los derechos, además asegurándose de incorporar procedimientos para verificar la identidad de los afectados. Por último, se tiene que cumplir el deber de publicidad de la información impuesto por la LTBG, aunque puede verse limitado en supuestos excepcionales en los que prima la seguridad y la intimidad.

Hay que tener en cuenta la importancia de la accesibilidad, una fácil consecución de la información prima en este sector para tener protegido el derecho de acceso de todas las personas, también la interoperabilidad tanto entre ciudadano y Administración como entre Administraciones entre sí para que fluyan los documentos solicitados y por supuesto debe primar la seguridad, por ejemplo, no sería oportuno otorgar la información solicitada por teléfono ya que es difícil comprobar de manera exhaustiva la identidad de la persona que habla.

### **3. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y PUBLICIDAD PASIVA**

#### **a) Notas básicas de la evolución comunitaria de la normativa sobre protección de datos de carácter personal<sup>10</sup>**

En el año 2016 se aprobó el RGPD, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, entró en vigor a los 20 días de su publicación pero se le dio un plazo de adaptación hasta el 25 de mayo de 2018 en el que ya será vinculante en toda la UE. Su contenido, al ser un Reglamento, es directamente aplicable, pero como es muy genérico debido a que esta

---

<sup>10</sup> Véase CAZURRO BARAHONA, V., “Introducción a la protección de datos personales” punto 1, en *Grandes Tratados. Practicum protección de datos 2015*, BIB 3509, enero 2014. Véase SUBIRANA DE LA CRUZ, S., “Open government: transparencia administrativa, derecho de acceso a la información pública, “open data” y reutilización de la información en el sector público” punto III y V, en *Revista Aranzadi doctrinal*, nº 2, 2016.



aplicabilidad debe darse en todos los Estados pertenecientes a la Unión Europea se necesita, al menos en España, una ley que lo haga más específico a nuestro sistema y que solucione aquellos puntos que se contradicen con nuestra antigua LOPD y su Reglamento de desarrollo, por tanto, ese es el cometido de nuestro legislador en el actual ALOPD.

En primer lugar es interesante hacer referencia a la evolución comunitaria en materia de protección de datos, la primera vez que aparece en Europa el derecho a mantener la vida privada es en el artículo 8 del Convenio Europeo de los Derechos Humanos (Roma 1950)<sup>11</sup>. En el Convenio número 108 del Consejo de Europa (1981) se señala la protección de las personas respecto de sus datos teniendo en cuenta la intromisión de la informática (muy desfasado debido a la época). Posteriormente en el artículo 8 de la Carta de los Derechos Fundamentales de la UE (Estrasburgo 2007, aunque con entrada en vigor el 1 de diciembre de 2009) ya se habla de protección de datos de carácter personal<sup>12</sup>. Siguiendo esta línea, en el Tratado de Lisboa (2007) se añade en su número 16 que el Parlamento Europeo y el Consejo serán los encargados de establecer las normas que regularán la protección de datos. Sin embargo la más importante (sin tener en cuenta el RGPD) ha sido la Directiva 95/46/CE (24 de octubre de 1995) del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Por el RGPD se deroga la Directiva 95/46/CE, esta antigua Directiva, regulaba los mínimos para la protección de los datos y dejaba a los Estados Miembros más margen de decisión. Su objetivo era el mismo que el del RGPD, encontrar el equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la UE<sup>13</sup>. En ella, se exigía la creación de un organismo nacional independiente encargado de la supervisión de cualquier actividad relacionada con el tratamiento de los datos personales, en nuestro caso, la Agencia Española de Protección de Datos. Una de las principales diferencias con la normativa actual es que ésta sí que

---

<sup>11</sup> Véase MAYOR GOMEZ, R., “Contenido y novedades del Reglamento General de Protección de Datos en la UE” punto 2, en Gabilex, nº 6, 2016.

<sup>12</sup> “Artículo 8 Protección de datos de carácter personal 1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.”

<sup>13</sup> Véase DE MIGUEL ASENSIO, P., “Protección de Datos Personales” en Estudios y Comentarios legislativos, enero 2015.

permitía el consentimiento tácito<sup>14</sup>, lo cual se elimina fulminantemente con el nuevo Reglamento, además la Directiva regulaba únicamente los derechos ARCO (acceso, rectificación, cancelación y oposición), mientras que el Reglamento incluye dos más, derecho al olvido y a la portabilidad de los datos, lo cual desarrollaré posteriormente.

Se debe tener en cuenta que este Reglamento no regula el tratamiento de datos personales relativo a personas jurídicas, aunque se recoja el nombre, la forma de persona jurídica y sus datos de contacto (Considerando 14 RGPD). Tampoco de los datos de las personas fallecidas, aunque da la opción a sus herederos de disponer de ellos en cierta manera (Considerandos 27, 158 y 160 RGPD). En la LOPD se daba la opción a que las personas vinculadas con la persona fallecida pudieran dirigirse a los responsables de las actividades de tratamiento, acreditando la defunción, y solicitar la cancelación de los datos de éste. En el ALOPD se prevé en su artículo 3 (salvo que haya futuras modificaciones) una mayor regulación; ahora, después de certificar la muerte, podrán acceder a los datos, suprimirlos o rectificarlos, a no ser que existan limitaciones, tanto los herederos, como el albacea testamentario y en el caso de muerte de un menor o un discapacitado, podrán hacerlo también sus representantes legales, las personas designadas para su cuidado o el Ministerio Fiscal (de oficio o a instancia de cualquier interesado).

El RGPD surge por el tremendo desarrollo de la informática que nuestra sociedad está experimentando, las personas tenemos cada vez más facilidades a la hora de recopilar información y transmitirla, por ello, nace la necesidad de crear nuevas normas para su protección<sup>15</sup>. Con él se pretende unificar y modernizar la normativa europea sobre protección de datos, permitiendo a los ciudadanos controlar mejor sus propios datos. Su ámbito material, igual que el de la Directiva 95/46/CE, es tanto el tratamiento automatizado de datos (total o parcial), como el no automatizado que se almacena en ficheros, aunque se pretende que a corto-medio plazo nuestras Administraciones estén totalmente digitalizadas.

Es obligatorio en todos sus elementos para todos los establecimientos responsables o encargados de la Unión Europea independientemente de que el tratamiento de los datos

---

<sup>14</sup> Véase MORALES BARCELÓ, J., “Big Data y Protección de Datos: especial referencia al consentimiento de los afectados” puntos III y IV, en Revista Aranzadi de Derecho y nuevas tecnologías, nº 44, 2017.

<sup>15</sup> Véase TRONCOSO REIGADA, A., “Hacia un nuevo marco jurídico europeo de protección de datos personales” puntos II y V, en Revista Española de Derecho Europeo nº 43, 2012.

tenga lugar en la UE o no. También al tratamiento de los datos personales de residentes de la Unión cuando el responsable o encargado no está establecido en la UE, por lo que las empresas que tienen su sede fuera deberán aplicar estas reglas si ofrecen sus servicios aquí (artículo 3 RGPD).

Es importante tener en cuenta que, las disposiciones relativas a la Protección de Datos de carácter personal no serán de aplicación si los datos recogidos y almacenados, aunque sean relativos a personas concretas, estén tratados de tal manera que la información que se obtenga no pueda asociarse a persona identificada o identificable (considerando 26 RGPD). Por ejemplo, datos estadísticos relativos a grupos de personas sin identificar. Este procedimiento se denomina disociación de los datos, y permitirá su tratamiento sin someterse a las obligaciones y requisitos que la ley impone.

#### **b) Novedades que aporta el Reglamento General de Protección de Datos 2016/679** **16**

Sus novedades más características son<sup>17</sup>:

1. Se incorpora el principio de responsabilidad activa<sup>18</sup>, lo que significa que el responsable del tratamiento de los datos debe cumplir con los principios que señala el RGPD y ser capaz de demostrar dicho cumplimiento, estos principios consisten en que debe existir licitud, lealtad y transparencia, los datos deben estar actualizados y sobre todo se da mucha importancia al principio de minimización de datos, en el que se requiere que los datos personales sean adecuados y limitados sólo a lo necesario en relación a los fines para los que serán tratados, igual que su plazo de conservación que a diferencia de como ocurre ahora en España, sólo podrá dilatarse hasta que su finalidad haya sido cumplida, o hasta que finalice el tiempo de archivado que se señale

---

<sup>16</sup> ÁLVAREZ HERNANDO, J., “El Reglamento Europeo y la futura Ley General de Protección de Datos: sus principales novedades” en Aranzadi digital, nº 1, 2017.

Véase DE LA HERA JUSTICIA, Z., “El Reglamento General de Protección de Datos y su incidencia en la administración local” en La Administración práctica, nº 3, 2017.

<sup>17</sup> Véase MAYOR GOMEZ, R., “Contenido y novedades del Reglamento General de Protección de Datos en la UE” punto 3, en Gabilex, nº 6, 2016.

<sup>18</sup> Véase AEPD, guías sectoriales “Protección de datos y administración local”. Disponible en: [http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2018/Guia\\_Proteccion\\_Datos\\_Administracion\\_Local.pdf](http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2018/Guia_Proteccion_Datos_Administracion_Local.pdf) y PORTAL DE TRANSPARENCIA (Diputación de Almería), “Información sobre el derecho de acceso”. Disponible en: <http://www.dipalme.org/Servicios/cmsdipro/index.nsf/informacion.xsp?p=dipalme&documentId=154E46FC3B507BE8C1257FF0002C203D>

al interesado cuando éste otorgue el consentimiento. Todo ello va de la mano con la intención del RGPD de que la privacidad exista desde el diseño y por defecto (artículo 25.1 RGPD), lo que se pretende es proteger los datos desde las primeras fases, así evitar llegar al punto en que se produzcan fallos en la seguridad o tener que imponer medidas muy costosas para asegurar su preservación y confidencialidad, para ello proponen actuaciones como la seudonimización de los datos que es la anonimización de estos desde que se recogen y recoger la menos cantidad posible necesaria para el fin<sup>19</sup>. Se pretende evitar que se produzca el daño y después repararlo, el *modus operandi* consiste en tener los datos controlados desde que se produce la primera recogida.

2. Encontramos las notificaciones si se producen quiebras de seguridad que puedan afectar a los datos personales (artículos 33 y 34 RGPD)<sup>20</sup>, en el caso de que se produzca la destrucción, pérdida o alteración accidental o ilícita de los datos, o la comunicación o acceso no autorizado a éstos, el responsable del tratamiento debe comunicarlo si hay riesgo para los derechos y libertades de las personas físicas, tanto a la AEPD, en menos de 72 horas y a los afectados, cuando antes. Las evaluaciones de impacto (artículo 35 RGPD), cambian la forma en la que se distingue el nivel de seguridad que se da a cada actividad de tratamiento, ahora su configuración no va en función del nivel (bajo, medio y alto), sino que los responsables deben realizar una valoración del riesgo de los tratamientos para establecer las medidas de seguridad a aplicar en cada caso.
3. Otra de las novedades que incluye el RGPD como ya citaba en el epígrafe anterior, es la inclusión de dos nuevos derechos ejercitables por el interesado<sup>21</sup>, en concreto el derecho de supresión conocido como derecho al olvido (artículo 17 RGPD) gracias al

---

<sup>19</sup> RGPD 2016/679 Artículo 4 apartado 5 “«seudonimización»: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.”

<sup>20</sup> Véase AEPD, guías sectoriales “Protección de datos y administración local”. Disponible en: [http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2018/Guia\\_Proteccion\\_Datos\\_Administracion\\_Local.pdf](http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2018/Guia_Proteccion_Datos_Administracion_Local.pdf)

<sup>21</sup> Véase AEPD, guía “Los derechos para proteger los datos personales”. Disponible en: [http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/infografias/RGPD\\_Derechos\\_ciudadanos\\_AEPD.pdf](http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/infografias/RGPD_Derechos_ciudadanos_AEPD.pdf)

cual nace la opción de eliminar los datos personales propios siempre que no estén sujetos a ninguna limitación (por ejemplo si hay razones de interés público en el ámbito de la salud que lo impiden, si se necesitan para la formulación, el ejercicio o la defensa de reclamaciones etc.), también nace el derecho de portabilidad de los datos (artículo 20 RGPD) por el cual el interesado podrá pedir sus datos a un responsable de tratamiento y transferirlos a otro e incluso esta transferencia podrá realizarse de responsable a responsable si los medios lo permiten.

4. El Reglamento cambia la forma de dar el consentimiento (artículo 7 RGPD), ahora será libre, específico, informado, inequívoco y expreso<sup>22</sup>. Se debe poder demostrar que se ha prestado fehacientemente y que éste es válido. La inacción tal como se entendía en la Directiva 95/46/CE ya no es una forma de obtener el consentimiento, por tanto los consentimientos tácitos dejarán de ser válidos en el momento en que el RGPD entre en vigor, incluso para los tratamientos de datos iniciados con anterioridad. Si nos encontramos en el caso de que el consentimiento se requiere para varios fines pueden ser agrupados según su vinculación (por ejemplo si se consiente recibir información publicitaria, se distingue entre propia de la página en la que se encuentra el interesado e información publicitaria de terceros). Pero, en el caso de que los tratamientos conlleven conductas diferentes, por ejemplo un consentimiento conlleva que quienes han recogido los datos pueden tratarlos y el otro que éstos serán cedidos a terceros, en estos casos, no se pueden presentar de forma agrupada, sino que deben separarse distinguiéndose de forma inteligible, clara y sencilla. Por último, es muy importante que el consentimiento se pueda revocar con la misma facilidad con la que se concedió.
5. Por otro lado, este nuevo Reglamento suprime la inscripción de los antiguos ficheros, ahora llamados actividades de tratamiento, en la AEPD<sup>23</sup>. Aunque, los responsables

---

<sup>22</sup> Artículo 4 apartado 11 RGPD “«consentimiento del interesado»: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.”

Véase MAYOR GOMEZ, R., “Contenido y novedades del Reglamento General de Protección de Datos en la UE” en Gabilex, nº 6, 2016.

<sup>23</sup> Véase AEPD, guías sectoriales “Protección de datos y administración local”. Disponible en: [http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2018/Guia\\_Proteccion\\_Datos\\_Administracion\\_Local.pdf](http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2018/Guia_Proteccion_Datos_Administracion_Local.pdf)

y encargados deberán crear el Registro de Actividades de Tratamiento (artículo 30 RGPD), que es una especie de inventario de los datos que tratan, es decir, que están bajo su responsabilidad, indicando en él los elementos señalados en el Reglamento (por ejemplo los datos de contacto del responsable y del Delegado de Protección de Datos, la categorías de datos recogidos, los fines del tratamiento, si hay transferencia de datos, a quién, los plazos de supresión de éstos, etc.).

6. Se añaden nuevas categorías especiales de datos personales (artículo 9 RGPD), en general los datos de carácter especial son aquellos más sensibles que cuando constan en una actividad de tratamiento conllevan la consecuencia de tener que asignarle una mayor seguridad<sup>24</sup>. Además de los que ya existían antes de la llegada del Reglamento (origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, datos relativos a la salud o a la sexualidad, y las infracciones o condenas) se añaden nuevos como datos genéticos y biométricos, su tratamiento está prohibido siempre que su finalidad sea identificar de forma única a una persona<sup>25</sup>. Por ejemplo se utilizan datos biométricos en las empresas, es a lo que se le llama comúnmente “fichar”, dejar la huella antes de entrar y salir del puesto de trabajo, su finalidad está permitida por que es el control de que el trabajador cumple con sus obligaciones laborales.
7. Por último pero una de las mayores novedades, la figura del Delegado de Protección de Datos (artículos 37 a 39 RGDP), que lleva a cabo el tratamiento de datos a gran escala o de especial categoría, además de asesorar a los responsables y encargados de tratamiento en su actividad. Su perfil será el de una persona especializada en Derecho y con práctica en materia de protección de datos, deberá garantizar un tratamiento adecuado de los datos, será necesario tanto en Administraciones u organismos públicos, como en empresas privadas (aquellas que tengan más de 250 trabajadores o

---

<sup>24</sup> Véase MAYOR GOMEZ, R., “Contenido y novedades del Reglamento General de Protección de Datos en la UE” en Gabilex, nº 6, 2016.

<sup>25</sup> Artículo 4 apartado 13 RGPD “«datos genéticos»: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.”

Artículo 4 apartado 14 RGPD “«datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.”

empresas que aunque no tengan ese tamaño traten un gran volumen de datos o datos delicados como los de categoría especial o datos relativos a condenas e infracciones penales)<sup>26</sup>. El Delegado en ningún caso tendrá responsabilidad a título personal y sus funciones se basan en hacer un registro general de actividades de tratamiento, es decir, un inventario de su actividad en el que se detallará: qué datos se están tratando, para qué finalidad, a quiénes se le está transfiriendo, durante cuánto tiempo se conservan etc., además si la información recogida contiene datos que provocan un grave riesgo deberá realizarse un análisis de riesgos y una evaluación de impacto para determinar las medidas técnicas, organizativas, de seguridad y de cumplimiento normativo a seguir, que actualmente ya no son las del procedimiento de la LOPD en el que las medidas están muy tasadas y son siempre las mismas cuando se determina un nivel. Mar España, la Presidenta de la AEPD en las jornadas realizadas en el INAP llamadas "Proceso para la adaptación al reglamento general de protección de datos en las Administraciones públicas"<sup>27</sup>, habla sobre la figura del Delegado de Protección de Datos en el caso de España, un país que cuenta con una gran cantidad de pequeños municipios de menos de cinco mil habitantes, y señala que no será necesario tener uno por cada municipio, ya que éstos ni generan tanto datos ni tienen tal cantidad de recursos, sino que las Diputaciones Provinciales serán las que aporten su delegado para trabajar tanto en la diputación como en los municipios cercanos. Las universidades también necesitarán un Delegado de Protección de Datos. Habrá un registro de delegados pero en ellos no aparecerá su nombre propio en concreto sino sus datos de contacto.

---

<sup>26</sup> “Especial atención merecen las sanciones que la nueva normativa europea impone para el incumplimiento por parte del responsable y encargado del tratamiento de esta obligación de designar un delegado de protección de datos, y que pueden llegar hasta los diez millones de euros o, tratándose de una empresa, de una cuantía equivalente al 2% del volumen de negocio total anual global del ejercicio financiero anterior, optándose, además, por la que resulte de mayor cuantía de las dos.” GONZALEZ CALVO, M., “La nueva figura del Delegado de Protección de Datos”, *Actualidad Jurídica Aranzadi*, nº 939, 2018.

Véase GONZALEZ CALVO, M., “La nueva figura del Delegado de Protección de Datos” en *Actualidad Jurídica Aranzadi*, nº 939, 2018.

<sup>27</sup> Véase Jornada INAP "Proceso para la adaptación al reglamento general de protección de datos en las Administraciones públicas": <http://laadministraciondial.inap.es/noticia.asp?id=1508414>

### c) Grupo normativo interno actual o vigente<sup>28</sup>

La LOPD, ya citada anteriormente, es la normal actual sobre protección de datos que rige en España hasta que se apruebe definitivamente el ALOPD. Como antecedente, cabe destacar la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD), y que definió, por primera vez en España, los datos de carácter personal y la identificación del afectado. La LOPD se creó como contestación a la Directiva 95/46/CE y basa su articulado en el artículo 18 de la Constitución, en el que se asegura que nuestro ordenamiento jurídico restringirá el uso de la informática para asegurar a los ciudadanos sus derechos fundamentales de intimidad personal y familiar<sup>29</sup>. Ello sigue siendo igual en el Anteproyecto de Ley Orgánica de Protección de Datos que se ha propuesto, y continuará en la ley que se consolide, ya que el objetivo principal de la protección de datos es que cada persona tenga la seguridad de que sus datos se usan de forma adecuada, y que uno mismo tiene la potestad de controlarlos, consiguiendo con ello que no se puedan lesionar de ninguna manera nuestros derechos y libertades fundamentales. La mayor parte de la LOPD y su Reglamento de desarrollo estará desechado cuando sea definitivo el ALOPD, la parte que no se derogue convivirá con esta nueva norma.

Las cuestiones características de esta ley son<sup>30</sup>:

**1. La obligatoriedad de alta de los ficheros:** los ficheros son ahora llamados actividades de tratamiento, todos ellos debían ser inscritos en la AEPD (artículo 60 del Reglamento de Desarrollo de la LOPD, Real Decreto 1720/2007 de 21 de diciembre, en adelante RLOPD), en el caso de que fueran ficheros de titularidad pública debían publicarse previamente en el Boletín Oficial antes de inscribirse (artículos 20, 25 y 26 LOPD)<sup>31</sup>. Actualmente, siguiendo lo dispuesto por el RGPD, en el nuevo proyecto de Ley se señala que es suficiente con que el responsable del tratamiento cuente con un registro de

---

<sup>28</sup> Véase RUBIO TORRANO, E., “El Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal” en Revista doctrinal Aranzadi Civil-Mercantil, nº 1, 2018.

<sup>29</sup> Véase MORALES BARCELÓ, J., “Big Data y Protección de Datos: especial referencia al consentimiento de los afectados” en Revista Aranzadi de Derecho y nuevas tecnologías, punto IV apartado 1 (Regulación en la normativa española), nº 44, 2017.

<sup>30</sup> Véase DE MIGUEL ASENSIO, P., “Protección de Datos Personales” puntos 2 y 3, en Estudios y Comentarios legislativos, enero 2015.

<sup>31</sup> Véase ÁLVAREZ HERNANDO, J., “Obligaciones formales, inscripción, modificación y supresión de ficheros en el Registro General de Protección de Datos”, en Grandes Tratados. Practicum protección de datos 2015, BIB 3509, enero 2014.



actividades de tratamiento. Según Francisco Javier Sempere, uno de los ponentes en las ya citadas jornadas realizadas por el INAP llamadas "Proceso para la adaptación al reglamento general de protección de datos en las Administraciones Públicas", el hecho de que cuando entre en vigor el RGPD no se tengan que suscribir las actividades a la AEPD no significa en ningún caso desligarse de la Agencia, sino todo lo contrario ya que hoy en día las administraciones con las exigencias del nuevo reglamento tienen más trabajo que nunca, por ejemplo tendrán que seguir llevando a cabo comunicaciones con la AEPD cuando se produzcan brechas en la seguridad de los tratamientos además de en muchas otras ocasiones<sup>32</sup>.

**2. La existencia del documento de seguridad:** éste contiene toda la información de seguridad tanto de ámbito técnico como organizativo necesario para garantizar que los datos estaban a salvo y era de obligado cumplimiento tanto para las personas que tenían acceso a los sistemas de información como a los datos automatizados (artículo 9 LOPD). La seguridad es algo que ha cambiado mucho con las disposiciones de la UE; anteriormente, para cada fichero que entraba en la Administración se determinaba el riesgo teniendo en cuenta los datos recogidos. Tras esto, entraba en un nivel (bajo, medio o alto) y, una vez en el nivel todos los ficheros que se incluían tenían las mismas medidas. Actualmente, se sigue manteniendo, al menos en España, esta forma de agrupar los distintos tipos de actividades de tratamiento según su peligrosidad, es decir, por niveles, pero a cada una de las actividades de tratamiento se les hace una evaluación de impacto (artículo 35 RGPD) y así se establecen las medidas de seguridad específicas en cada caso. Lo que se sigue manteniendo de la antigua Ley es la obligatoriedad de tener actualizados los datos que están recogidos.

**3. El consentimiento de los afectados:** de nuestra antigua LOPD al RGPD hay un gran cambio aun manteniendo este requisito indispensable, y es que entonces era suficiente con obtener (en algunos casos) el consentimiento tácito del afectado (artículo 6 LOPD), sin embargo, ahora, es requisito imprescindible para la validez del consentimiento que éste sea expreso, inequívoco, informado y libre. Se prohíben las casillas pre marcadas en páginas web, se debe mostrar la configuración para el almacenamiento de "cookies" etc.

---

<sup>32</sup> Véase Jornada INAP "Proceso para la adaptación al reglamento general de protección de datos en las Administraciones públicas": <http://laadministraciondialdap.inap.es/noticia.asp?id=1508414>

Además, debe ser tan fácil otorgar el consentimiento como revocarlo y debe poder demostrarse que se ha obtenido. La edad de los menores para prestar el consentimiento continúa igual que en la LOPD, los menores de 14 años necesitan el consentimiento de los padres.

Actualmente en el RGPD igual que en la LOPD existen ciertos casos en los que no es necesario otorgar el consentimiento: si los datos se recogen porque se va a crear una relación contractual (ya que los datos son necesarios para su cumplimiento), si existe un interés legítimo del interesado (por ejemplo, un ciudadano se desmaya en la calle y es necesario dar sus datos a una ambulancia), si existe una obligación legal de darlos (por ejemplo cuando Hacienda solicita los datos personales para cumplir la obligación de pagar los tributos), si existe un interés público o si se solicitan en el ejercicio de poderes públicos (por ejemplo si un policía va a poner una multa y solicita los datos al conductor), si hay interés de terceros (por ejemplo si hay un golpe en un parking pero el causante se da a la fuga, en este caso el perjudicado podría solicitar los videos al parking para conocer la matrícula del coche).

**4. Niveles de seguridad:** las medidas de seguridad en la LOPD se regulaban en nivel bajo, medio y alto. Eran acumulativas con lo cual, cada nivel tenía sus medidas predeterminadas y se iban añadiendo conforme los datos exigían un nivel mayor<sup>33</sup>. Se establecen atendiendo a la mayor o menor necesidad de garantizar la confidencialidad e integridad de la información. En general, todos los ficheros que contenían datos de carácter personal ya gozaban con un nivel básico de seguridad, si contenían datos relativos a la comisión de delitos o infracciones un nivel medio, y si lo que se recogía en ellos eran datos ideológicos, de religión, creencias, origen racial, salud o vida sexual tenían un nivel alto. Si el responsable tenía una cantidad de datos de la persona suficiente como para realizarle una evaluación de personalidad, lo que es llamado un perfil, también se protegían con un nivel medio de datos aunque todo esto podría variar si hay una disposición específica. Actualmente, con el RGPD esto se pierde en parte, la esencia de los niveles continúa para llevar una línea de actuación parecida a la que se tenía con anterioridad de la entrada del reglamento, pero ahora no hay medidas prefijadas sino que

---

<sup>33</sup> Para saber más sobre las medidas de seguridad de cada nivel ir al Reglamento de Desarrollo de la LOPD, Real Decreto 1720/2007 Capítulo III y IV (nivel básico, medio y alto) para datos automatizados y no automatizados.

se realiza un análisis de riesgos y se determina las medidas necesarias para cada conjunto de datos recogidos.

**5. Derechos ARCO:** se compone de los derechos que aún mantiene el RGPD (aunque éste incluye dos más, derecho de supresión y de portabilidad de los datos). Derecho de acceso (posibilidad del interesado de solicitar sus propios datos ante cualquier empresa u organismo, artículo 15 LOPD), derecho de rectificación y cancelación (rectificar los datos personales ante cualquier empresa u organismo además de poder cancelarlos cuando estén erróneos o sean inadecuados o excesivos, lo que se consigue es el bloqueo de los datos, no como con el nuevo derecho de supresión que los elimina, artículo 16) y derecho de oposición (con él se consigue que no se traten los datos o que se deje de hacerlo si el interesado no ha prestado su consentimiento, por ejemplo, impedir la recepción de publicidad no solicitada, artículo 17 LOPD)<sup>34</sup>.

#### **4. EJERCICIO DEL DERECHO DE ACCESO Y LÍMITES DERIVADOS DE LA TUTELA DE DATOS PERSONALES**

En un mundo como el nuestro en el que predomina la tecnología y la información, el acceso a los datos personales tiene restringirse para asegurar el cumplimiento de los derechos fundamentales. Debe existir un equilibrio entre la libre circulación de la información y el derecho a la intimidad y la protección de datos, se debe tener siempre muy presente el principio de proporcionalidad. Por otro lado, aparece la transparencia, que es una obligación de los Estados de dar publicidad de sus actuaciones, ello también es limítrofe con la protección de datos ya que se tiene que encontrar una manera de que las Administraciones y sus órganos sean transparentes sin perjudicar a la privacidad los individuos.

La protección de datos, la transparencia y el derecho de acceso son pesas de una balanza y hay que ponderar cuándo pesa más una que las otras.

Algunos autores como J. L. Piñar Mañas critican el modo en que nuestra LTBG configura el derecho de acceso ya que la creación de una nueva ley era la oportunidad perfecta para

---

<sup>34</sup> Existe un servicio llamado Listas Robinson en el que las personas que no desean recibir información (telefónica, postal, por correo o por SMS) se apuntan y toda empresa y organismo debe conocer esta información y respetarla. Para más información: <https://www.listarobinson.es/>

redibujar el derecho de acceso como un derecho fundamental y no como mera parte de la transparencia<sup>35</sup>. En la actualidad nuestro derecho de acceso es un derecho de configuración legal diseñado sobre el mandato al legislador que contiene el artículo 105 b) de la Constitución.

#### **a) Procedimiento<sup>36</sup>**

El derecho de acceso puede ejercitarse como reconoce la LTBG por “todas las personas”, por lo que se incluye a personas físicas y a jurídicas<sup>37</sup>, presentando una solicitud en forma de formulario establecido (artículo 17 LTBG)<sup>38</sup>, ello puede ser bien por la vía electrónica, a través de la página del organismo administrativo al que se quiera dirigir en el apartado “transparencia” que conduce al interesado al portal de transparencia correspondiente en cada caso, en él encontraremos una pestaña llamada “solicite información”, para ello habrá que identificarse electrónicamente tanto si se actúa en nombre propio como si es en representación de otra persona, con la identificación se pretende conocer la identidad de la persona, qué información solicita y los datos de contacto para efectuar las comunicaciones<sup>39</sup>. O bien, de forma presencial, del mismo modo deberán rellenar un

---

<sup>35</sup> Véase PIÑAR MAÑAS, J. L., “Transparencia y derecho de acceso a la información pública, algunas reflexiones en torno al derecho de acceso en la Ley 19/2013 de Transparencia, Acceso a la información pública y Buen Gobierno” en Revista catalana de dret públic, nº 49, 2014.

<sup>36</sup> Véase RAMS RAMOS, L., “El procedimiento de ejercicio del derecho de acceso a la información pública” en Revista General de Derecho Administrativo, nº 41, 2016.

Véase COMENTARIO A LA LTBG, BIB 210, enero 2017.

<sup>37</sup> Véase ÁLVAREZ HERNANDO, H., CAZURRO BARAHONA, V., “Ejercicio de los derechos ARCO. Derecho al olvido en internet” punto 7, en Grandes Tratados. Practicum protección de datos 2015, BIB 3509, enero 2015.

Véase PORTAL DE TRANSPARENCIA (Gobierno de España), “Guía para el ciudadano del derecho de acceso a la información”. Disponible en:

<http://transparencia.gob.es/transparencia/dam/jcr:eb071b8f-7982-4518-b102-d2a4f5f51640/guia-del-ciudadano.pdf>

<sup>38</sup> El formulario para ejercitar el derecho de acceso a información pública puede encontrarse en la página web de transparencia del gobierno de España ([http://transparencia.gob.es/transparencia/transparencia\\_Home/index.html](http://transparencia.gob.es/transparencia/transparencia_Home/index.html)) como en la página de cada comunidad autónoma en su sección de transparencia, para Andalucía (<https://ws043.juntadeandalucia.es/derechodeacceso/tramites/acceso.do?jsessionid=C5D07FDF36F0A9716B6AEBA8474F116E?vertodos>) y en otros organismos como Diputaciones, por ejemplo la Diputación de Almería (<http://www.dipalme.org/Servicios/cmsdipro/index.nsf/informacion.xsp?p=dipalme&documentId=671A62A2667B3B3EC1257D03003FBFD0>).

<sup>39</sup> Véase PORTAL DE TRANSPARENCIA (Gobierno de España), “Guía para el ciudadano del derecho de acceso a la información”. Disponible en:

<http://transparencia.gob.es/transparencia/dam/jcr:eb071b8f-7982-4518-b102-d2a4f5f51640/guia-del-ciudadano.pdf> y PORTAL DE TRANSPARENCIA (Diputación de Almería), “Información sobre el derecho de acceso”. Disponible en:

formulario y aportar sus datos (puede ser en los registros de los órganos administrativos a los que se dirijan, en los de cualquier órgano administrativo que pertenezca a la Administración General del Estado, de las Comunidades Autónomas o de las Diputaciones Provinciales, Cabildos y Consejos Insulares etc.). El solicitante debe señalar el modo en el que prefiere que se le envíe la información para la que ha solicitado el acceso. El interesado puede conocer en cualquier momento el estado de su solicitud entrando en el portal con sus claves. El sistema de claves es muy sencillo y aporta mucha seguridad. El ciudadano puede identificarse a través de un usuario y contraseña, su DNI-e o con un certificado electrónico.

Cuando se solicita la información no es obligatorio expresar la finalidad, pero los motivos pueden ser tenidos en cuenta cuando se dicte la resolución, aunque la falta de éstos nunca será causa de rechazo de la solicitud (artículo 17.3 LTBG)<sup>40</sup>. Esto es así porque no es un requisito legal para la aprobación de la solicitud, pero sin embargo si existieran ciertas dudas sobre si la petición es repetitiva o no, y se demuestra un interés legítimo, no cabrá posibilidad de rechazo, o si estamos ante el caso de un tipo de información de acceso limitado en las que según el artículo 14.2 LTBG habrá que ponderar la finalidad de la petición con los intereses en juego, la motivación jugará un papel relevante.

Si la solicitud ha sido dirigida a un órgano que no es el que posee dicha información, se remitirá ésta al órgano competente, en el caso de que no lo conozca se informa de este hecho al solicitante. Igualmente se le comunicará si la información que pide no se considera lo suficientemente concretada y si el interesado no contesta en 10 días se entiende que desiste. Si lo que solicita afecta a terceros (límite del derecho de acceso con

---

<http://www.dipalme.org/Servicios/cmsdipro/index.nsf/informacion.xsp?p=dipalme&documentId=154E46FC3B507BE8C1257FF0002C203D>

<sup>40</sup> Acerca de la previsión legal de concurrencia de un interés público o «privado» del solicitante, Emilio GUICHOT señala que “el derecho de acceso no es un derecho instrumental al servicio de la protección de otros derechos, sino un derecho autónomo al servicio de la transparencia, la participación y el control de la actuación pública, conectado con el Estado democrático y, por ende, al margen de cualquier distinción en función de la motivación que pueda tener el solicitante. Dicho de otro modo, el único parámetro con el que confrontar la protección de los límites es el valor que para la sociedad tiene el conocimiento de la información, un juicio abstracto desvinculado por completo de la cualidad y motivación del solicitante.” GUICHOT REINA, E., Transparencia, Acceso a la Información Pública y Buen Gobierno: Estudio de la Ley 19/2013, Revista de Estudios de la Administración Local y Autonómica: Nueva Época, nº 2, 2014.

la protección de datos) éstos tienen un plazo de 15 días para realizar alegaciones y mientras se suspende el procedimiento (artículo 19 LTBG).

El plazo máximo para conceder o denegar la solicitud es de un mes desde la recepción de ésta y debe notificársele al interesado y a los terceros afectados<sup>41</sup>. El plazo puede prorrogarse un mes más en caso necesario, si hay un número muy elevado de solicitudes, si el volumen de la información es muy grande, si la dificultad de la misma lo hace indispensable etc. Deberá notificársele previamente al interesado e indicar los motivos del retraso. Todas las resoluciones que denieguen el acceso, que lo acepten pero parcialmente o en un modo distinto al que se pidió y las que concedan el acceso aunque se haya producido la oposición de un tercero estarán motivadas, tanto en la ponderación de intereses como sobre las cuestiones planteadas. En el caso de que se supere el plazo establecido como máximo, si no se ha dictado ni notificado una resolución, se entiende que ese silencio es una respuesta y por lo tanto la solicitud quedará desestimada (artículo 20 LTBG). En mi opinión que exista la desestimación por silencio en una petición de este tipo no es muy justo porque por un lado la LTBG señala que las resoluciones deberán ser motivadas pero luego regula posibilidad de que quepa un rechazo sin ninguna explicación, ello además lleva a que existan más reclamaciones ya que el interesado en obtener la información quiere llegar hasta el final del caso, conocer el motivo de la desestimación y luchar por la consecución de los datos. Sin embargo, aunque no lo considero del todo acertado sí que es mejor que en la regulación anterior de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (en adelante LRJAP) en la que se entendía el silencio como que se concedía el acceso a dicha información, ya que así se puede evitar que la Administración otorgue por error las informaciones.

Ante la admisión de la solicitud se producirá la formalización del acceso (artículo 22 LTBG), que siempre será por vía electrónica a no ser que no haya sido posible o se haya

---

<sup>41</sup> “Es muy posible que este plazo sea mayor dado que el mismo no empieza a contar hasta que el órgano competente para resolver recibe la solicitud. Esto significa que si ésta se presenta ante otro órgano, el plazo no empezará a correr hasta que en cumplimiento de lo dispuesto en el artículo 19.1 LTBG se dé traslado de la misma al órgano que se considera competente.” RAMS RAMOS, L., “El procedimiento de ejercicio del derecho de acceso a la información pública” punto 4, en Revista General de Derecho Administrativo, nº 41, 2016.

solicitado otro método. La notificación de la resolución se debe dar en un plazo de no más de diez días.

Si la resolución es desestimatoria caben una serie de recursos. Estas resoluciones sobre el acceso a la información pública serán recurribles ante la jurisdicción Contencioso-administrativa<sup>42</sup>, sin perjuicio de la posibilidad de interponer la reclamación de carácter potestativo y previa a la interposición de los recursos prevista en el artículo 24 ante el Consejo de Transparencia y Buen Gobierno (para reclamaciones ante órganos o entidades de carácter estatal ya que las autonómicas y locales serán ante el órgano independiente que estas determinen, a no ser que le atribuyan su competencia al CTBG), sustitutiva de los recursos administrativos (artículos 20.5 y 23.1 LTBG).

- El recurso contencioso-administrativo se interpone mediante un escrito contra la Administración para actos que pongan fin a la vía administrativa, para casos de inactividad de la administración o para actuaciones consideradas no legales que ésta presuntamente ha cometido. El plazo para presentarlo será de dos meses si el acto es expreso, es decir, si se recibe una respuesta denegatoria, y de 6 meses si el acto es presunto, contando desde el día siguiente al que el hecho se produce. Posteriormente, si procede se llevara a cabo el emplazamiento de los demandados y la admisión del recurso y una vez presentada la demanda, hechas las alegaciones y pruebas, y en su caso, celebrada la vista y expuestas las conclusiones, la sentencia debidamente motivada se dictará en el plazo de diez días desde que se concluya el pleito, excepto si no es posible que se pondrá otra fecha y se comunicará a los interesados (artículos 45 a 73 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa).
- Recurso ante el Consejo de Transparencia y Buen Gobierno (desde ahora CTBG) es un organismo independiente encargado de promover el cumplimiento de la obligación de transparencia pública, velar por el derecho de acceso a la

---

<sup>42</sup> Según el artículo 2.1.f ) LTBG “Sólo cabe la interposición de recurso contencioso-administrativo contra las resoluciones dictadas por la Casa de su Majestad el Rey, el Congreso de los Diputados, el Senado, el Tribunal Constitucional y el Consejo General del Poder Judicial, así como el Banco de España, el Consejo de Estado, el Defensor del Pueblo, el Tribunal de Cuentas, el Consejo Económico y Social y las instituciones autonómicas análogas, en relación con sus actividades sujetas a Derecho Administrativo”.

información y garantizar la observancia de las disposiciones de buen gobierno<sup>43</sup>. Tiene personalidad jurídica propia y capacidad de obrar plena tanto pública como privada.

Sus funciones consisten en: hacer cumplir de la mejor manera la LTBG por la que se rige, asesorar en sus principales materias (transparencia, derecho de acceso y buen gobierno), informar los proyectos normativos del Estado que tengan relación con la LTBG, evaluar la aplicación efectiva de ésta ley y a finales de cada año presentar una memoria sobre su cumplimiento ante las Cortes Generales, y que también se publica para la información de los ciudadanos, crear directrices sobre buenas prácticas para el desarrollo de éstas materias, promover actividades de formación, como podrían ser cursos, sensibilizar a la gente sobre la importancia del conocimiento de las nombradas materias y por último colaborar con otros órganos que también trabajen estos temas.

Las personas que han solicitado una información (ya sea de competencia estatal, autonómica o local) y no se les haya respondido, se les haya respondido pero no se les ha facilitado la información o simplemente no estén conformes con la respuesta, podrán reclamar al CTBG (artículo 24.6 LTBG). Las reclamaciones pueden ser: de forma presencial en su sede, por correo postal, en un registro público o electrónicamente, es decir, accesible para todos.

El plazo para su resolución es de un mes desde el día siguiente que se recibe la respuesta o desde el día siguiente al que se termina el periodo para recibirla y no se le ha contestado (artículo 24.2 LTBG) y las resoluciones dictadas por el Consejo, serán publicadas en la página web y en el Portal de Transparencia, sin datos personales de los intervinientes ya que se someten a una disociación previa para protegerlos<sup>44</sup>. El plazo del Consejo para resolver y notificar será de tres

---

<sup>43</sup> Véase ENÉRIZ OLAECHEA, F. J., “Los órganos externos encargados de resolver las reclamaciones por denegación de acceso a la información pública: Consejos de Transparencia” en Revista Aranzadi doctrinal, nº 5, 2018.

<sup>44</sup> Véase la página del CTBG apartado “recursos y jurisprudencia” [http://www.consejodetransparencia.es/ct\\_Home/Actividad/recursos\\_jurisprudencia/Recursos\\_AGE/2018/79\\_MSanidad\\_4.html](http://www.consejodetransparencia.es/ct_Home/Actividad/recursos_jurisprudencia/Recursos_AGE/2018/79_MSanidad_4.html) recurso 14 de diciembre de 2017 nº de referencia 0437/2017 sobre “Las productividades abonadas a los empleados públicos y funcionarios desde 2016” (En este caso se solicita dicha información al Ministerio de Sanidad, Servicios Sociales e Igualdad



meses, de lo contrario se entiende que se ha desestimado el recurso (artículo 24.4 LTBG), ésta resolución tiene carácter ejecutivo y contra ella solo se podrá interponer recurso contencioso-administrativo.

#### **b) Denegación de acceso e información de acceso limitado<sup>45</sup>**

Como apunta J. L. Piñar Mañas<sup>46</sup>, las excepciones al derecho de acceso a la información, al “right to know”, deben ser limitadas y estar previstas en la ley ya que esa información pertenece a los ciudadanos, además las excepciones deben estar basadas en daños identificables, no abstractos, y éste daño debe ser superior al interés público que se atiende otorgando la información. Las personas tenemos derecho a conocer las actuaciones de los poderes públicos, la motivación de éstas, el uso que se hace de los fondos públicos etc.

Los límites al acceso a la información se basan en que ésta pueda suponer un perjuicio (artículo 14 LTGB)<sup>47</sup>: para el Estado en el sentido de la seguridad nacional, la defensa, las relaciones exteriores y la seguridad pública<sup>48</sup>. También en el caso de que pueda afectar al funcionamiento de los poderes públicos en la prevención, investigación y sanción de los ilícitos penales, administrativos o disciplinarios<sup>49</sup>. Si la comunicación de cierta

---

pero éste no la facilita basándose en que existe un procedimiento específico de acceso a la información, contenido en el Estatuto Básico del Empleado Público (EBEP) por lo que se presenta un recurso ante el CTBG y éste lo concede parcialmente ya que no existe dicho procedimiento pero entiende que dar toda esa información puede vulnerar el derecho a la protección de datos de carácter personal).

<sup>45</sup> Véase RAMS RAMOS, L., “El procedimiento de ejercicio del derecho de acceso a la información pública” punto 4, en Revista General de Derecho Administrativo, nº 41, 2016. Véase MORETÓN TOQUERO, A., “Los límites del derecho de acceso a la información pública” en Revista jurídica de Castilla y León, nº 33, mayo 2014.

<sup>46</sup> Véase PIÑAR MAÑAS, J. L., “Transparencia y derecho de acceso a la información pública, algunas reflexiones en torno al derecho de acceso en la Ley 19/2013 de Transparencia, Acceso a la información pública y Buen Gobierno” en Revista catalana de dret públic, nº 49, 2014.

<sup>47</sup> Véase AEPD, “Criterio interpretativo: aplicación de los límites al derecho de acceso a la información”, 24 de junio de 2015. Disponible en:

[https://www.agpd.es/portalwebAGPD/canaldocumentacion/criterios\\_art\\_15/common/Criterio\\_CTBG-AEPD\\_24-6-2015\\_2.pdf](https://www.agpd.es/portalwebAGPD/canaldocumentacion/criterios_art_15/common/Criterio_CTBG-AEPD_24-6-2015_2.pdf)

Véase PORTAL DE TRANSPARENCIA (Gobierno de España), “Guía para el ciudadano del derecho de acceso a la información”. Disponible en:

<http://transparencia.gob.es/transparencia/dam/jcr:eb071b8f-7982-4518-b102-d2a4f5f51640/guia-del-ciudadano.pdf>

<sup>48</sup> Véase resolución denegatoria nº de expediente 001-002493 Ministerio de Interior sobre “información sobre listado de empresas, filiales o compañías que hayan sido declaradas como infraestructuras críticas (se deniega el acceso porque está clasificado como **secreto**)” <http://www.interior.gob.es/documents/10180/2894648/001-002493.pdf>

<sup>49</sup> Véase resolución denegatoria nº de expediente 001-004004 Ministerio de Interior sobre “informe del cuerpo nacional de policía” (se deniega el acceso porque se solicitaba información sobre la compatibilidad de unas empresas que tenía un comisario de la policía, pero como ello

información pudiera afectar a la igualdad de las partes en los procesos judiciales y la tutela judicial efectiva<sup>50</sup>, a las funciones administrativas de vigilancia, inspección y control<sup>51</sup>, a los intereses económicos y comerciales o a la política económica y monetaria<sup>52</sup>. Tampoco se pueden compartir informaciones que colisionen con el secreto profesional y la propiedad intelectual e industrial<sup>53</sup>, o la garantía de la confidencialidad o el secreto requerido en procesos de toma de decisión<sup>54</sup>. Por último, se prohíbe también si es perjudicial para la protección del medio ambiente<sup>55</sup>. Esto es así porque si ciertas informaciones se divulgasen podría provocar inseguridad, entorpecimiento del normal funcionamiento de la Administración, perjuicio a individuos en concreto, etc.

---

podría suponer que comience un procedimiento de oficio y se creara un expediente disciplinario y esta información formaría parte de él no se puede otorgar) <http://www.interior.gob.es/documents/10180/2894648/001-004004.pdf>

<sup>50</sup> Véase resolución denegatoria nº expediente 001-001882 Ministerio de Hacienda y Administraciones Públicas sobre “identificación de los sujetos acogidos a la amnistía fiscal” (se deniega el acceso porque los datos de carácter tributario son reservados y solo pueden utilizarse para aplicarse tributos y sanciones y no cederse a terceros) [http://www.minhfp.gob.es/Documentacion/Publico/GobiernoAbierto/Transparencia\\_Denegatorias/001-001882\\_Denegatoria.pdf](http://www.minhfp.gob.es/Documentacion/Publico/GobiernoAbierto/Transparencia_Denegatorias/001-001882_Denegatoria.pdf)

<sup>51</sup> Véase resolución denegatoria nº expediente 001-005607 Ministerio de Economía y Competitividad sobre “programa de seguimiento radiológico y sanitario de la población de palomares entre 1966 y 2015” (se deniega el acceso porque la información que se pedía podía perjudicar las funciones del Centro de terrenos contaminados de Palomares, sin embargo no lo deniega totalmente porque ofrece al interesado la posibilidad de acceder al informe de caracterización radiológica) <http://transparencia.gob.es/transparencia/dam/jcr:69d9dca9-b080-4bb9-aea2-beaba0fc34dd/Resolucion-005223-005607-MINECO.pdf>

<sup>52</sup> Véase resolución denegatoria nº expediente 001-010550 Ministerio de Fomento sobre “el número de maquinistas y trenes gestionado por RENFE” (en este caso se deniega solo parte de la información ya que la de RENFE mercancías no puede trasladarse al interesado porque podría dañar sus intereses económicos y comerciales) [http://www.fomento.gob.es/RESOLUCIONESDENEGATORIAS/001-010550\\_resolucion\\_concesion\\_parcial\\_art.14.1.h.pdf](http://www.fomento.gob.es/RESOLUCIONESDENEGATORIAS/001-010550_resolucion_concesion_parcial_art.14.1.h.pdf)

<sup>53</sup> Véase resolución denegatoria nº expediente 001-007455 Ministerio de Educación, Cultura y Deporte sobre “Memoria de la Universidad de Córdoba para la Verificación del Plan de Estudios de la titulación de Graduado en Relaciones Laborales y Recursos Humanos” (se deniega el acceso porque contiene datos personales, aunque no especialmente protegidos, y sobre todo porque forma parte de la propiedad intelectual de esta universidad) <http://www.mecd.gob.es/dms/mecd/transparencia/resoluciones/001-007455/001-007455.pdf>

<sup>54</sup> Véase la resolución denegatoria nº expediente 001-006709 Ministerio de Empleo y Seguridad Social sobre “La cotización a la Seguridad Social de un Alcalde (se deniega el acceso ya que los datos obtenidos por la administración de la Seguridad Social en sus funciones son reservados) [file:///C:/Users/porbi/Downloads/1a-Resoluci%C3%B3n-001-006709-009503\\_csv.pdf](file:///C:/Users/porbi/Downloads/1a-Resoluci%C3%B3n-001-006709-009503_csv.pdf)

<sup>55</sup> Véase la resolución denegatoria nº expediente 001-006759 Ministerio de Defensa sobre “la información del Ministerio de Defensa del Medio Ambiente” (se deniega el acceso porque la divulgación de estas informaciones podría suponer un perjuicio para el medio ambiente, aunque se le concede parte de la información que solicita como cuál es la estructura del Ministerio, la normativa ambiental que ha desarrollado etc.) <http://transparencia.gob.es/transparencia/dam/jcr:a617ef93-58a2-4951-bd61-c84a8328891a/Resolucion-006759-MDEF-anonimizada.pdf>

Pero, este artículo no supondrá la exclusión automática del derecho a la información ya que según este mismo artículo la aplicación de estos límites dependerá del caso concreto, se ponderará si existe un interés público o privado que sea superior al test de daño que justifique el acceso a la información, esto es comprobar el perjuicio que supone el acceso a una determinada información sobre el interés que pretende proteger la confidencialidad. La Ley exige que sea un daño y no un simple peligro. Incluso también se puede dar la posibilidad de un acceso parcial a la información señalando al interesado la parte de la información que ha sido omitida previa disociación de los datos de carácter personal que estuvieren incluidos.

Si la información solicitada constara de datos especialmente protegidos también se considera información de acceso limitado<sup>56</sup>. En el artículo 7.2 de la LOPD nos encontramos a qué se refiere claramente el legislador con el término “Datos especialmente protegidos”, también en el artículo 9 del RGPD (aunque incluye dos nuevos, los datos genéticos y biométricos) y son: “los datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física.” El legislador señala (artículo 15 LTBG) que para su acceso deberá existir expreso consentimiento del afectado por escrito a no ser que él mismo ya haya hecho manifiestamente públicos sus datos.

En el caso del apartado 3 del artículo 7 de la LOPD, nos encontramos ante datos relativos a la comisión de infracciones penales o administrativas que no conlleven la amonestación pública al infractor, en este caso sólo se puede dar acceso a estas informaciones en caso de que se cuente con el consentimiento expreso del afectado o si se estuviera amparado por una norma con rango de Ley.

---

<sup>56</sup> Véase MORETÓN TOQUERO, A., “Los límites del derecho de acceso a la información pública” en Revista jurídica de Castilla y León, nº 33, mayo 2014.

Si se realiza una petición de información y ésta contiene datos identificativos pero no especialmente protegidos, el órgano debe realizar una ponderación teniendo en cuenta el interés público, el menor perjuicio y la garantía de los derechos de los afectados y la justificación o motivación de la petición por los solicitantes. Todo ello a no ser que los datos sean disociados previamente.

El CTBG nos arroja un poco de luz con su criterio interpretativo 2/2015 de estas limitaciones al derecho de acceso señalando que para la aplicación de los artículo 14 y 15 de la LTBG habrá que: 1) Valorar si la información solicitada contiene o no datos de carácter personal; 2) Si es así, comprobar si existen datos especialmente protegidos y si existen sólo se podrán conceder si hay consentimiento expreso del afectado o si el supuesto está amparado por una norma con rango de Ley; 3) Si no son datos especialmente protegidos, valorar si son o no exclusivamente datos meramente identificativos relacionados con la organización, el funcionamiento o la actividad pública del órgano o entidad correspondiente y entonces facilitarlos a no ser que prevalezca en los casos individuales la protección de datos de carácter personal u otros derechos constitucionales; 4) Si los datos no fueran exclusivamente identificativos, relacionados con la organización, el funcionamiento o la actividad pública del órgano o entidad se deben ponderar tal como señala el artículo 15 apartado 3 LTBG; y 5) Por último observar si se dan los límites que permiten la denegación del acceso previa realización de un test de daño y un test de interés público (artículo 14 LTBG) <sup>57</sup>.

Por lo tanto ninguno de los límites regulado por la LTBG operan automáticamente ya que se debe aplicar de acuerdo a las reglas y los elementos de ponderación. Se debe motivar y justificar la denegación, cabe la posibilidad de acceso parcial y todas las resoluciones denegatorias serán objeto de publicidad.

---

<sup>57</sup> Test de daño: analizarse si la estimación de la petición de información supone un perjuicio concreto, definido y evaluable.

Test de interés público: aplicación justificada y proporcional atendiendo a la circunstancia del caso concreto y siempre que no exista un interés que justifique la publicidad o el acceso.

### c) Inadmisión de acceso

Se puede producir una inadmisión a trámite de la solicitud (artículo 18 LTBG)<sup>58</sup>. Dicha inadmisión se puede dar por varios motivos:

- Si la información está en curso de elaboración o publicación general, por lo tanto en cuanto esto se lleve a cabo será parte de la publicidad activa y no será necesario solicitarla. Se inadmite el acceso para salvaguardar la eficacia de la actuación administrativa. Son informaciones inconclusas sobre las que se está trabajando, no tienen nada que ver con documentos de un procedimiento administrativo que aún no ha concluido, igualmente en este último caso también se permite generalmente su acceso. En este caso, las mayoría de las Comunidades Autónomas, pero concretamente Andalucía ha concretado la causa de inadmisión señalando en su Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía (en adelante LTPA), que la denegación deberá especificar qué órgano elabora la información y el tiempo que aproximadamente llevará su inclusión en los portales de transparencia (artículo 30.a).
- Si la información tiene carácter auxiliar, de apoyo etc. como por ejemplo borradores, notas, etc. En esta misma LTPA se considera que los informes preceptivos no pueden ser considerados información auxiliar, aun así se deja gran discrecionalidad para considerar qué clase de información pertenece a este tipo ya que el artículo no es *numerus clausus*<sup>59</sup>.

---

<sup>58</sup> Véase COMENTARIO A LA LTBG, BIB 210, enero 2017.

<sup>59</sup> Véase el criterio interpretativo del CTBG 6/2015, en él se explica que no son sólo las informaciones denominadas notas, borradores etc. sino que lo que importa es el tipo de información que se incluye en ellas y especifica que: “Una petición puede ser inadmitida a trámite cuando se den, entre otras, alguna de estas circunstancias: 1 Que contengan valoraciones personales u opiniones del autor que no manifiesten la posición de un órgano o entidad; 2 Cuando se solicite un texto preliminar o borrador sin la consideración de final; 3 Cuando se trate de información preparatoria de la actividad del órgano o entidad que recibe la solicitud; 4 Cuando la solicitud se refiera a comunicaciones internas que no constituyan trámites del procedimiento; 5 Cuando se trate de informes no preceptivos y que no sean incorporados como motivación a una decisión final.” Por lo cual lo que es relevante y no se puede denegar son aquellas informaciones que son relevantes en la tramitación del expediente y en la conformación de la voluntad del órgano. Por último, este criterio señala que la causas de inadmisión previstas en el artículo 18 de la LTBG se deben interpretar de forma restrictiva y aplicarse de forma motivada. <http://www.consejodetransparencia.es/ct/Home/Actividad/criterios.html>

- Si la información necesita una reelaboración previa para que pueda ser divulgada. En mi opinión, este motivo de inadmisión es bastante abierto ya que no señala qué información es la que necesita ser reelaborada ni el plazo que la persona que la solicita tendrá que esperar para que le sea otorgada<sup>60</sup>.
- Si la solicitud se ha dirigido a un órgano que no tenga la información e ignore quién es el órgano competente. Ya que si conociera qué órgano lo debe resolver lo remitirá a éste siempre informando de ello al interesado (artículo 19 LTBG). Desde mi punto de vista es difícil para un ciudadano de a pie afrontar la compleja estructura de la Administración sin fallos, por lo tanto debería ser ésta la que se encargara de encontrar el órgano al que compete resolver dicha solicitud y así dar cumplimiento al derecho de acceder a la información que se nos otorga por ley. Además, el artículo 20 de la LTBG señala que los plazos para resolver la solicitud sólo comenzarán a contar desde que la misma es recibida por el órgano competente, por lo tanto, este error puede dilatar el procedimiento mucho más de lo conveniente y perjudicar al ciudadano. Por otro lado, uno de los principios de las Administraciones Públicas es la interoperabilidad, el traslado de información de unas a otras de forma rápida y ágil, sin embargo en este caso delegan esta carga en el ciudadano dificultando, desde mi punto de vista, este sencillo proceso.
- Si la información es manifiestamente repetitiva o tiene un carácter abusivo no justificado con la finalidad de la Ley de Transparencia<sup>61</sup>. La petición será infundada

---

<sup>60</sup> Véase el criterio interpretativo del CTBG 7/2015, en él se explica que el concepto de reelaboración no es la mera agregación, o suma de datos, o el mínimo tratamiento de los mismos sino que según esta interpretación es la que deba: “a) Elaborarse expresamente para dar una respuesta, haciendo uso de diversas fuentes de información, o b) Cuando dicho organismo o entidad carezca de los medios técnicos que sean necesarios para extraer y explotar la información concreta que se solicita, resultando imposible proporcionar la información solicitada.” Además el CTBG aclara que los supuestos de información de gran volumen o complejidad que amplían el plazo de entrega no son reelaboración (sólo puede darse en algunos casos determinados si a consecuencia del gran volumen debe reelaborarse), tampoco la información que debe ser anonimizada es reelaborada, ni en el caso del artículo 19.4 LTBG cuando la información es propiedad de un órgano en concreto pero se encuentra distribuida en otros órganos, y por último, sí que se puede considerar reelaboración a la necesidad de que la administración aporte la información en un formato que no posee siempre que suponga un nuevo tratamiento de la información.

[http://www.consejodetransparencia.es/ct\\_Home/Actividad/criterios.html](http://www.consejodetransparencia.es/ct_Home/Actividad/criterios.html)

<sup>61</sup> Véase el criterio interpretativo del CTBG 3/2016, en el que se explica que se trata de dos casos diferentes: solicitud manifiestamente repetitiva (1 Ya presentada una o más veces anteriormente por el o los mismos solicitantes y denegada de manera firme por incurrir en

o se considerará excesiva si se ejercita en plazos inferiores a 12 meses sin tener un interés legítimo, si se puede considerar como repetitiva, etc., entonces el responsable podrá cobrar un precio razonable por la información, o negarse a aportarla. En estos casos el responsable siempre deberá poder demostrar la repetitividad manifestada. Se viene a referir al principio general de buena fe y no abuso que existe en todo el ordenamiento jurídico español. Esto tampoco puede dar paso a que cualquier petición que sea más trabajosa de las que se reciben comúnmente sea rechazada, puesto que entonces estaríamos ante un caso de abuso por parte de la administración<sup>62</sup>.

Por lo tanto, los motivos de inadmisión a trámite están un poco indeterminados y necesitan de interpretación, esta debe ser llevada a cabo de forma restrictiva para no denegar toda petición que se reciba y poder brindar las posibilidades que otorga el derecho de acceso.

---

alguno de los límites de los artículos 14 y 15 LTBG o en alguna causa de inadmisión del artículo 18 de la misma ley; 2 Petición ya concedida anteriormente a los solicitantes y sin que haya ninguna modificación en los datos desde entonces; 3 Que los solicitantes conozcan el sentido de la resolución porque ya se le había comunicado en un procedimiento anterior; 4 Que la petición coincida con otra ya realizada y que aún no se haya resuelto; 5 Cuando fueran de respuesta imposible y se haya informado al solicitante) y carácter abusivo de la petición de información (siempre en sentido cualitativo porque la cantidad de peticiones sobre temas diferentes no implica un ejercicio abusivo del derecho, es abusiva cuando lo es su intención u objeto, cuando de ser atendida obligue a parar el resto de la gestión de los sujetos obligados a dar la información, cuando suponga un riesgo para los derechos de los terceros y cuando sea contrario a las normas, las costumbres y la buena fe. Por otro lado no estará justificada con la finalidad de la ley si no se puede reconducir a ninguna de las finalidades de ésta, si su objetivo es obtener información considerada como no pública y si su posible consecuencia sea la comisión de un ilícito. [http://www.consejodetransparencia.es/ct\\_Home/Actividad/criterios.html](http://www.consejodetransparencia.es/ct_Home/Actividad/criterios.html)

<sup>62</sup> Véase STSJ Valencia, Sección 1ª, de 2 de enero de 2001 en la que una ciudadana solicita al Ayuntamiento una copia diligenciada del expediente completo de aplicación de contribuciones especiales para la ejecución del proyecto de obras. El Ayuntamiento rechaza la solicitud porque ello supondría la paralización de su actividad. Y el Tribunal estimó el recurso porque no se acreditó que la excesiva información solicitada hubiera afectado en alguna medida a la eficacia del funcionamiento de los servicios públicos.

## CONCLUSIONES

- I. El derecho de acceso y el derecho de protección de datos no son derechos fundamentales, sino derechos de configuración legal, pero en la evolución de la sociedad se están convirtiendo en materias muy importantes ya que son temas que sin darnos cuenta tratamos cada día, por ejemplo damos permiso a una aplicación del teléfono móvil para tratar nuestros datos, le solicitamos una recopilación de ellos a un órgano de la Administración Pública, etc. Probablemente, en un futuro no tan lejano el derecho de acceso a la información y el derecho de protección de los datos de carácter personal serán tan importantes como cualquiera de los derechos fundamentales que hoy en día conocemos.
- II. Nuestra normativa al respecto se ha modernizado mucho a lo largo de los años, sobre todo gracias a la presión que ejerce sobre nosotros la Unión Europea que es mucho más pionera en este sector. La legislación no ha sido muy permanente en este tema ya que cambia al tiempo que nuestra sociedad y que los avances tecnológicos, hace tan solo cincuenta años teníamos una regulación muy primitiva y sin embargo actualmente existen normas estatales, Directivas, Reglamentos Europeos, etc.
- III. El modelo de actuación ha cambiado y aunque ahora también se le da importancia a la seguridad en las nuevas regulaciones, prima más que el proceso de recogida cuente con la mínima cantidad de datos y sean recogidos y archivados de la forma más anónima posible para evitar problemas futuros que invertir en medidas protectoras y de seguridad o reparadoras en el caso de que el daño ya se haya producido, la idea es adelantarse a las quiebras de seguridad y así evitarlas.
- IV. Es una materia que abarca tantos sectores que tiene una gran cantidad de trabajo, a pesar de que el RGPD fuese aprobado en 2016 y se diesen dos años para su adaptación (hasta el 25 de mayo de 2018) en España aún hay esferas en las que mejorar, al menos en el sector público, ya que ha cambiado su modo de operar casi completamente en lo que a éste ámbito se refiere. Desde mi experiencia, tras realizar las prácticas curriculares en la Excma. Diputación de Almería y dedicarme de lleno a la adaptación a las nuevas normas, he comprobado cómo hemos tenido que modificar, entre otras cosas, todos los formularios que se expedían en todos los ámbitos para cumplir con la nueva normativa y, sobre todo, evitar recoger datos innecesarios.



- V. El derecho de acceso ante el que nos encontramos es universal, lo que quiere decir que todas las personas pueden acceder a él (tanto físicas como jurídicas) y se observa en él una amplia discrecionalidad ya que aunque en la ley se regulan muchos motivos que pueden suponer su limitación pero todos ellos deben ponderarse teniendo en cuenta el caso concreto. Hay que poner siempre en una balanza la transparencia, el derecho de acceso, el interés público y la protección de datos para obrar en el sentido que menos perjudique sin ser excesivamente restrictivos.
- VI. La gran diferencia del RGPD con su predecesora, la Directiva 95/46/CE, es que ya no se da esa amplio margen de elección a los Estados Miembros, sino que ahora las normas son del todo impositivas ya que éste tema se ha vuelto muy relevante en los últimos años, además de la seguridad que esto aporta aunque siga existiendo esa movilidad de los datos. Todo ello sin olvidar las grandes sanciones previstas en el Reglamento en caso de incumplimientos.
- VII. El RGPD supone un antes y un después en la protección de datos de carácter personal, aún más tras escándalos tan sonados como la sanción que ha impuesto la AEPD a empresas privadas de la magnitud de WhatsApp o Facebook por la cesión de millones de datos a terceros sin el consentimiento de los afectados, ahora las personas comienzan a darse cuenta de la importancia que de tener el control y que exista seguridad sobre sus datos.
- VIII. En mi opinión, lo más importante es que la gente conozca cuáles son sus derechos para poder salvaguardar los datos, tener claro que éstos no pueden ser tratados sin nuestro consentimiento expreso (salvo casos previstos en la Ley) y que tenemos la posibilidad de revocarlo si así lo deseamos en un momento dado.

## BIBLIOGRAFÍA

- GAMERO CASADO, E., FERNÁNDEZ RAMOS, S., MORA RUIZ, M., Tema 11 “El estatuto del ciudadano. La posición jurídica del ciudadano: transparencia y acceso a la información pública, el derecho de protección de los datos personales” en *Derecho Administrativo para estudios no jurídicos*, Tecnos, Madrid, 2016.
- PÉREZ ROYO, J., Lección 12 “Los derechos constitutivos de la personalidad: honor, intimidad y propia imagen”, lección 13 “Los derechos de la comunicación física, intelectual y social: libertad de expresión”, lección 25 “El Gobierno: transparencia y acceso de los ciudadanos a la Administración” en *Curso de Derecho Constitucional*, Marcial Pons, Madrid, 2016.
- SOTO LOSTAL, S., Capítulo III “Derecho de acceso a la información de los archivos y registros de la administración pública”, Capítulo IV “Derecho de acceso a los archivos y registros administrativos como especialidad del derecho a recibir información veraz por cualquier medio de difusión” en *Derecho de acceso a la información*, Tirant lo Blanch, Valencia, 2011.

### Artículos de revistas:

- ÁLVAREZ HERNANDO, H., CAZURRO BARAHONA, V., “Ejercicio de los derechos ARCO. Derecho al olvido en internet” en *Grandes Tratados. Practicum protección de datos 2015*, BIB 3509, enero 2015.
- ÁLVAREZ HERNANDO, J., “El Reglamento Europeo y la futura Ley General de Protección de Datos: sus principales novedades” en *Aranzadi digital*, nº 1, 2017.
- ÁLVAREZ HERNANDO, J., “Obligaciones formales, inscripción, modificación y supresión de ficheros en el Registro General de Protección de Datos”, en *Grandes Tratados. Practicum protección de datos 2015*, BIB 3509, enero 2014.
- BALLESTEROS, R., “Nueva Ley 39/2015 y derecho de acceso a los expedientes administrativos” en *Actualidad jurídica Aranzadi*, nº 923, 2016.
- CAZURRO BARAHONA, V., “Introducción a la protección de datos personales” en *Grandes Tratados. Practicum protección de datos 2015*, BIB 3509, enero 2014.
- COMENTARIO A LA LTBG, BIB 210, enero 2017.
- DE MIGUEL ASENSIO, P., “Protección de Datos Personales” en *Estudios y Comentarios legislativos*, enero 2015.
- DE LA HERA JUSTICIA, Z., “El Reglamento General de Protección de Datos y su incidencia en la administración local” en *La Administración práctica*, nº 3, 2017.
- ENÉRIZ OLAECHEA, F. J., “Los órganos externos encargados de resolver las reclamaciones por denegación de acceso a la información pública: Consejos de Transparencia” en *Revista Aranzadi doctrinal*, nº 5, 2018.

- FERNÁNDEZ RAMOS, S., “Acceso a la información pública versus protección de datos personales” en *Revista española de Derecho Administrativo*, nº 184, 2017.
- GONZALEZ CALVO, M., “La nueva figura del Delegado de Protección de Datos” en *Actualidad Jurídica Aranzadi*, nº 939, 2018.
- GUICHOT REINA, E., Transparencia, Acceso a la Información Pública y Buen Gobierno: Estudio de la Ley 19/2013, *Revista de Estudios de la Administración Local y Autonómica: Nueva Época*, nº 2, 2014.
- MAYOR GOMEZ, R., “Contenido y novedades del Reglamento General de Protección de Datos en la UE” en *Gabilex*, nº 6, 2016.
- MORALES BARCELÓ, J., “Big Data y Protección de Datos: especial referencia al consentimiento de los afectados” en *Revista Aranzadi de Derecho y nuevas tecnologías*, nº 44, 2017.
- MORETÓN TOQUERO, A., “Los límites del derecho de acceso a la información pública” en *Revista jurídica de Castilla y León*, nº 33, mayo 2014.
- PIÑAR MAÑAS, J. L., “Transparencia y derecho de acceso a la información pública, algunas reflexiones en torno al derecho de acceso en la Ley 19/2013 de Transparencia, Acceso a la información pública y Buen Gobierno” en *Revista catalana de dret públic*, nº 49, 2014.
- RAMS RAMOS, L., “El procedimiento de ejercicio del derecho de acceso a la información pública” en *Revista General de Derecho Administrativo*, nº 41, 2016.
- RUBIO TORRANO, E., “El Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal” en *Revista doctrinal Aranzadi Civil-Mercantil*, nº 1, 2018.
- SUBIRANA DE LA CRUZ, S., “Open government: transparencia administrativa, derecho de acceso a la información pública, “open data” y reutilización de la información en el sector público” en *Revista Aranzadi doctrinal*, nº 2, 2016.
- TRONCOSO REIGADA, A., “Hacia un nuevo marco jurídico europeo de protección de datos personales” en *Revista Española de Derecho Europeo* nº 43, 2012.

### **Material complementario:**

#### **Guías:**

- AEPD, “Criterio interpretativo: aplicación de los límites al derecho de acceso a la información”, 24 de junio de 2015. Disponible en: [https://www.agpd.es/portalwebAGPD/canaldocumentacion/criterios\\_art\\_15/commo n/Criterio\\_CTBG-AEPD\\_24-6-2015\\_2.pdf](https://www.agpd.es/portalwebAGPD/canaldocumentacion/criterios_art_15/commo n/Criterio_CTBG-AEPD_24-6-2015_2.pdf)
- AEPD, guías sectoriales “Protección de datos y administración local”. Disponible en: [http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/G uías/2018/Guía\\_Proteccion\\_Datos\\_Administracion\\_Local.pdf](http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/G uías/2018/Guía_Proteccion_Datos_Administracion_Local.pdf)

- AEPD, guía “Adaptación al RGPD, Administraciones Públicas”. Disponible en: [http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/infografias/Adaptacion\\_RGPD\\_AAPP.pdf](http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/infografias/Adaptacion_RGPD_AAPP.pdf)
- AEPD, guía “Los derechos para proteger los datos personales”. Disponible en: [http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/infografias/RGPD\\_Derechos\\_ciudadanos\\_AEPD.pdf](http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/infografias/RGPD_Derechos_ciudadanos_AEPD.pdf)
- INAP, “Estudio comparado sobre normativa interna en materia de derecho de acceso a la información pública”, Madrid, 2016.
- PÉREZ CAMBERO, R., guía sobre normativa comentada, “Cómo adecuarse a las exigencias del Reglamento General de Protección de Datos”, en *Actualidad Administrativa*, núm. 11, noviembre 2017.
- PORTAL DE TRANSPARENCIA (Gobierno de España), “Guía para el ciudadano del derecho de acceso a la información”. Disponible en: <http://transparencia.gob.es/transparencia/dam/jcr:eb071b8f-7982-4518-b102-d2a4f5f51640/guia-del-ciudadano.pdf>
- PORTAL DE TRANSPARENCIA (Diputación de Almería), “Información sobre el derecho de acceso”. Disponible en: <http://www.dipalme.org/Servicios/cmsdipro/index.nsf/informacion.xsp?p=dipalme&documentId=154E46FC3B507BE8C1257FF0002C203D>
- PORTAL DE TRANSPARENCIA (Diputación de Almería), “Solicitud de información pública”. Disponible en: <http://www.dipalme.org/Servicios/Organizacion/servicios.nsf/xFicha.xsp?ref=400000-SV-800201>

#### **Vídeos:**

- Jornada INAP "Proceso para la adaptación al reglamento general de protección de datos en las Administraciones públicas": <http://laadministracionaldia.inap.es/noticia.asp?id=1508414>

#### **Leyes utilizadas:**

- ANTEPROYECTO DE LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE 26 DE OCTUBRE DE 2017, disponible en: [http://www.congreso.es/backoffice\\_doc/prensa/notas\\_prensa/57631\\_1518684517278.PDF](http://www.congreso.es/backoffice_doc/prensa/notas_prensa/57631_1518684517278.PDF)
- CONSTITUCIÓN ESPAÑOLA, disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229>  
Además de la sinopsis de los artículos disponible en la página del Congreso de los Diputados: <http://www.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=20&tipo=2>

- DIRECTIVA 95/46/CE (24 DE OCTUBRE DE 1995) DEL PARLAMENTO EUROPEO Y DEL CONSEJO, RELATIVA A LA PROTECCIÓN DE LAS PERSONAS FÍSICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES Y A LA LIBRE CIRCULACIÓN DE ESTOS DATOS, (derogada) disponible en:  
<http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM:114012>
- LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS, disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750>  
Además de la página de: <https://ayudaleyprotecciondatos.es/2017/06/27/lopd-2018/>
- LEY ORGÁNICA 5/1992, DE 29 DE OCTUBRE, DE REGULACIÓN DEL TRATAMIENTO AUTOMATIZADO DE LOS DATOS DE CARÁCTER PERSONAL, disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-A-1992-24189>
- LEY 29/1998, DE 13 DE JULIO, REGULADORA DE LA JURISDICCIÓN CONTENCIOSO-ADMINISTRATIVA, disponible en:  
<https://www.boe.es/buscar/act.php?id=BOE-A-1998-16718>
- LEY 30/1992, DE 26 DE NOVIEMBRE, DE RÉGIMEN JURÍDICO DE LAS ADMINISTRACIONES PÚBLICAS Y DEL PROCEDIMIENTO ADMINISTRATIVO COMÚN (derogada), disponible en:  
<https://www.boe.es/buscar/doc.php?id=BOE-A-1992-26318>
- LEY 19/2013, DE 9 DE DICIEMBRE, DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y BUEN GOBIERNO, disponible en:  
<https://www.boe.es/buscar/doc.php?id=BOE-A-2013-12887>
- LEY 1/2014, DE 24 DE JUNIO, DE TRANSPARENCIA PÚBLICA DE ANDALUCÍA, disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-2014-7534&p=20141231&tn=2>
- LEY 39/2015, DE 1 DE OCTUBRE, DEL PROCEDIMIENTO ADMINISTRATIVO COMÚN DE LAS ADMINISTRACIONES PÚBLICAS, disponible en:  
<https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565>
- REGLAMENTO DE DESARROLLO DE LA LOPD, REAL DECRETO 1720/2007 DE 21 DE DICIEMBRE, disponible en:  
<https://www.boe.es/buscar/act.php?id=BOE-A-2008-979>
- REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS DE LA UNIÓN EUROPEA 2016/679 de 27 de abril, disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679>

#### **Formación previa sobre protección de datos en las prácticas externas:**

- SOLER HERNÁNDEZ, M., DIPUTACIÓN DE ALMERÍA, curso sobre Protección de Datos Personales, LOPD y adecuación al RGPD UE. “Gestión de la Protección de Datos Personales en la Diputación de Almería y RPC”. *Servicio de organización y*

*Seguridad*, noviembre 2017 (Manual entregado sólo a los asistentes al curso, no disponible online).

**Información adicional:**

- PORTAL DEL CONSEJO DE TRANSPARENCIA Y BUEN GOBIERNO, disponible en: [http://www.consejodetransparencia.es/ct\\_Home/index.html](http://www.consejodetransparencia.es/ct_Home/index.html)